Protection of Personal Data in sub-Saharan Africa

Alex Boniface Makulilo

Protection of Personal Data in sub-Saharan Africa

Vom Fachbereich Rechtswissenschaft der Universität Bremen

angenommene

DISSERTATION

zur Erlangung des akademischen Grades

DOCTOR JURIS

(Dr. jur.)

vorgelegt

von Alex Boniface Makulilo

geboren am 17.08.1976 in Kigoma, Tanzania

Gutachter: Prof. Dr. Benedikt Buchner

Prof. Dr. Christoph Ulrich Schmid

Tag der Verteidigung : 25.10.2012, Bremen

Table of Contents

Abbreviations and Acronyms

ACHPR	African Charter on Human and Peoples' Rights
AIDS	Acquired immune deficiency syndrome
AJOL	African Journals Online
APEC	Asia-Pacific Economic Cooperation
Art	Article
AU	African Union
BPO	Business Process Outsourcing
CAT	Court of Appeal of Tanzania
CDHRI	Cairo Declaration on Human Rights in Islam
CETS	Council of Europe Treaty Series
CFI	Court of First Instance (EU)
CFR	Charter of Fundamental Rights (Europe)
CoE	Council of Europe
CRID	*Centre de Recherches Informatique et Droit* (University of Namur, Belgium)
CRS	Congressional Research Service
DAAD	Deutscher Akademischer Austausch Dienst
e.g.	*exampli gratia* (for example)
EAC	East African Community
EC	European Community
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECOWAS	Economic Community for West African States
ECtHR	European Court of Human Rights
ed(s)	editor
EEA	European Economic Area
EPIC	Electronic Privacy Information Centre
et al.	*et alii/alia* (and others)
etc	*et cetera* (extra)
ETS	European Treaty Series
EU	European Union
HCT	High Court of Tanzania
HIV	Human immunodeficiency virus

i.e.	*id est.* (that is to say)
Ibid	ibidem (in the same place)
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICT	Information Communication Technology
IMF	International Monetary Fund
Infra	later cited
ITES	Information Technology Enabled Service
MCT	Media Council of Tanzania
NEPAD	New Partnership for Africa's Development
No	Number
NRCCL	Norwegian Research Centre for Computers and Law
O.J	Official Journal of the European Communities/European Union
OAU	Organisation of African Unity
OECD	Organisation for Economic Co-operation and Development
OIC	Organisation of Islamic Cooperation
p/pp	page(s)
para	paragraph
PMG	Parliamentary Monitoring Group (South Africa)
R	Recommendation
RSA	Republic of South Africa
s	section
SA	South Africa
SADC	Southern African development Community
SAP	Structural Adjustment Programme
SH/SHA	Safe Harbor Agreement
Supra	previously cited
T.L.R	Tanzania Law Report
TCRA	Tanzania Communications Regulatory Authority
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UKHL	United Kingdom House of Lords
UN	United Nations
UNISA	University of South Africa

UNSW	University of New South Wales
URT	United Republic of Tanzania
US/USA	United States of America
USSR	Union of Soviet Socialist Republics
v	versus
Vol.	Volume
WB	World Bank
WIPO	World Intellectual Property Organisation
WITS	University of Witwatersrand
WLR	Weekly Law Report (UK)
WTO	World Trade Organisation

Acknowledgements

The completion of this thesis owes to the assistance I received from different individuals and organisations. I am particularly indebted to my supervisor Professor Dr. Benedikt Buchner. His early support in May 2009, particularly through acceptance to act as my supervisor, was the basis for fulfilment of the criteria for the scholarship award I secured to stay and research in Germany. Moreover, throughout the conduct of this research project, Professor Buchner provided me with invaluable academic and intellectual support. His constructive critical comments and advice shaped and reshaped my thoughts in this accomplishment. Similarly, I cast my sincere thanks of gratitude to Professor Dr. Christoph Ulrich Schmid who offered me the second supervision. His critical and constructive comments enlightened me to reach this far.

Prior to the commencement of this study, I received enormous support in the form of advice, comments and suggestions from various professors. I am deeply indebted to Professor Lee A. Bygrave of the University of Oslo, Norway. He was the first professor I discussed with him the initial proposal to carry out this project. Our discussion at *Domus Biblioteca* in Oslo in spring 2006 provided me with motivation and impetus to research in data privacy in Africa. Moreover, as my former professor at the University of Oslo, Bygrave wrote numerous recommendation letters in support of my applications for admission and finance to different universities.

I also wish to thank in a particular way Professor Roger Magnusson of the University of Sydney, Australia. I came to know Professor Magnusson in 2007 through email exchange. I worked my four drafts of the initial research proposal with Professor Magnusson. I have to admit, through his critical comments I had to revise and enrich my proposal to an acceptable standard. Apart from that, he gave me tips and advice on how to marshal and integrate relevant legal sources in my project. I will never forget his piece of advice that 'law theses are largely self-driven'. This piece of advice was of great motivation to me yet challenging in this endeavour. I would also like to cast similar expressions of gratitude to Professor J.E.J (Corien) Prins of the Tilburg University, The Netherlands. Initially, Professor Prins accepted to act as my supervisor but due to financial constrains I could not make this study at Tilburg. I am indebted to her, particularly on our meeting in Addis Ababa, Ethiopia in 2007 during the World IT Forum (WITFOR). We had discussions about my research proposal and issues of privacy and data protection generally. I received similar support from Professor Ian Walden of Queen Mary, University of London. I met Professor Walden in London in 2006 and we shared some discussions about data protection

in Africa. Later in 2008, Professor Walden offered me critical yet constructive comments on my proposal. It is interesting to mention that Professor Walden was at that time working as an expert for the development of Cyber law framework in East Africa. Other professors who offered their support in the form expressed above include Professor Serge Gutwirth (Vrije Universiteit Brussel); Professor Graham Greenleaf(University of New South Wales, Australia); Professor Peter Blume(University of Copenhagen, Denmark); Professor Paul de Hert(Tilburg University, The Netherlands); Dr. Anton Vedder(Tilburg University, The Netherlands); and Professor Spiros Simitis(Universität Frankfurt am Main).

During field research in South Africa, I received enormous support from Professors Iain Currie (University of Witwatersrand) and Anneliese Roos (University of South Africa). Apart from responding to my questions during interviews, they facilitated my access to other respondents and resources. I extend similar thanks to Mrs. Drudeisha Madhub, the Commissioner of Data Protection in Mauritius. She was very helpful not only in answering my interview questions but also in facilitating my access to the Library of the Supreme Court of Mauritius. I also thank Mr. R. Ranjit Dowlutta, the Clerk of the National Assembly in Mauritius. He made available to me the Hansards comprising of the transaction of the enactment of the Data Protection Act 2004 in Mauritius. My thanks are also due to Mr. Richard Kayumbo, Head of Department Consumer Affairs, Tanzania Communications Regulatory Authority and Mr. Adam Mambi, Assistant Secretary and Head of Legal Research Department, Law Reform Commission of Tanzania. They responded to my interviews and provided me with valuable resources.

In a special way, I thank Dr. Alexander B. Makulilo of the Department of Political Science and Public Administration, University of Dar es Salaam in Tanzania. He provided me with practical tips on how to handle a multi-disciplinary research. I am grateful to his invaluable contribution. Apart from that, Dr. Makulilo made some useful comments on the initial drafts of my research proposal and has also proof read the manuscript of this thesis. I am equally thankful to Ms. Victoria Makulilo, Mr. Erick Gabriel and Ms. Helen Kiunsi for proof reading the manuscript of this thesis.

My thanks are also due to Ms. Petra Wilkins as well as Ms. Kerstin True-Biletski. They handled all administrative and logistical arrangements that were necessary for carrying out my project. I am grateful to both of them for ensuring conducive research environment for this project to sail through.

My parents, Mr. Boniface Makulilo and Ms. Maria Moris have provided me continued support of various forms in my academic endeavours. They deserve my heartedly thanks.

I would also like to thank Mr. Nathaniel Mjema. I met him at the O.R Tambo International Airport, Johannesburg, just at the time of exiting on my arrival on 28 June 2011. Mr. Mjema offered me to stay with his family in Pretoria during the period of my field research in South Africa. He also assited me locating various research destinations and arrange some appointments. I am grateful for his generosity and support.

During my leisure time I used to meet Mr. Nasser Grandjean, his wife Petra and their daughter Lara. I enjoyed the social conversations and practical jokes we had, particularly with Lara. I am grateful and indebted to their support which re-energised me every time I got tired of writing this thesis. I equally extend much thanks to Mr. Paul Wabike and his family who live in Groningen, The Netherlands. I used to make visits there and refresh, particularly during holidays. Thank you!

For individuals and institutions whose names are not specifically mentioned here because they preferred anonymity, I owe them tribute. The information I collected from them was equally important in the analyses of this study.

Finally, I thank the DAAD for providing financial support of this research. My stay in Germany and research would have not been possible had it not been for this support. The financial support I received from my employer, the Open University of Tanzania, was invaluable towards covering field research costs. I am grateful to this support as well as the study leave.

Abstract

Africa is by far the least developed continent in terms of protection of personal data. At present there are 11 countries out of 54 which have implemented comprehensive data privacy legislation. Nine of them namely, Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Mauritius, Senegal and Seychelles belong to sub-Saharan Africa. The other two countries, Morocco and Tunisia, belong to North Africa. Yet, there are seven countries in sub-Saharan Africa with either Bills or drafts on data privacy pending before their respective legislative or executive bodies. These include Ivory Coast (Cote d'Ivoire), Kenya, Madagascar, Mali, Niger, Nigeria and South Africa. The rest of African countries have neither Bills nor drafts of such laws. The dominant discourse on privacy and data protection advances the 'culture of collectivism' as the reason for the state of privacy and regulation in Africa. Founded on the normative assumptions of the old debates engraved in universalism and cultural relativism, the main argument held in this discourse is that Africa's collectivism denies an individual a space to advance claims for privacy. The present study sought to interrogate this dominant discourse and in particular investigating the emerging trends of adopting comprehensive data privacy legislation in Africa. To avert from the inherent pitfalls of normative assumptions, this study engaged a hybrid methodology. It triangulated the doctrinal, empirical and international comparative law methodologies. Moreover, in order to gain in-depth insights of the state of privacy, the study delimited to three sub-Saharan African countries: Mauritius, South Africa and Tanzania as cases. Based on documents collected and interviews held, this study has found that although collectivist culture is an important factor in explaining the limited state of privacy in Africa, it is not a catch-all phenomenon. Instead, technological, economic, political and social processes have significantly affected privacy consciousness and consequently the systems of privacy and data protection in the continent.

Table of Statutes and Conventions

African Union

Addis Ababa Declaration on Information and Communication Technologies in Africa: Challenges and Prospects for Development 2010

African Charter on Human and Peoples' Rights 1981

African Charter on the Rights and Welfare of the Child 1990

Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, Version 01/01.2011

Angola

Lei nº 22/11 Da Protecçao de Dados Pessoais 2011

APEC

APEC Privacy Framework 2004

Australia

Australian Privacy Amendment (Private Sector) Act 2000

Benin

Loi n° 2009-09 Portant Protection des Données à Caractère Personnel 2009

Burkina Faso

Loi n° 010-2004/AN Portant Protection des Données à Caractère Personnel 2004

Cameroon

Constitution of Cameroon 1996

Cape Verde

Cape Verdean Constitution 2010

Lei nº 133/V/2001, de 22 de Janeiro Regime Jurídico Geral de Protecção de Dados Pessoais a Pessoas Singulares 2001

Council of Europe

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981

Council of Europe Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine 1997

European Convention on Human Rights and Fundamental Freedoms 1950

World Health Organisation Declaration on the Promotion of Patients' Rights in Europe 1994

EAC

Draft Bill of Rights for the East African Community 2009

Legal Framework for Cyberlaws 2008 (Phase I)

Legal Framework for Cyberlaws 2011 (Phase II)

Treaty for Establishment of the East African Community 1999

ECOWAS

ECOWAS Treaty 1975

Supplementary Act A/SA.1/01/07 on the Harmonization of Policies and the Regulatory Framework for the Information and Communication Technology (ICT) Sector 2007

Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS 2010

European Union

Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows 2001

Charter of Fundamental Rights of the European Union 2000

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002

Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006

Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

General Data Protection Regulation 2012

Protocol No.11 (ETS No. 155) to the European Convention on Human Rights 1998

R (2010)13 with regard to automatic processing of personal data in the context of profiling 2010

R (81) 1 on regulations for automated medical data banks 1981

R (83) 10 on the protection of personal data used for scientific research and statistics 1983

R (2002) 9 on the protection of personal data collected and processed for insurance purposes 2002

R (85) 20 on the protection of personal data used for the purposes of direct marketing 1985

R (86) 1 on the protection of personal data for social security purposes 1986

R (87) 15 regulating the use of personal data in the police sector 1987

R (89) 2 on the protection of personal data used for employment purposes 1989

R (90) 19 on the protection of personal data used for payment and other operations 1990

R (91) 10 on the communication to third parties of personal data held by public bodies 1991

R (95) 4 on the protection of personal data in the area of telecommunication services 1995

R (97) 18 on the protection of personal data collected and processed for statistical purposes 1997

R (97) 5 on the protection of medical data 1997

R (99) 5 for the protection of privacy on the Internet 1999

Regulation (EC) 45/2001 with regard to the processing of personal data by the institutions and bodies on the Community 2001

Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws 2009

Treaty Establishing a Constitution for Europe 2004

Treaty of Lisbon 2007

Gabon

Loi n°001/2011 Relative à la Protection des Données à Caractère Personnel 2011

Ghana

Data Protection Act 2012

Ireland

Data Protection Act 1988

Freedom of Information Act 1997

Kenya

Constitution of Kenya 1963

Constitution of Kenya 2010

League of Arab States

Arab Charter of Human Rights 2004

Liberia

Freedom of Information Act 2010

Mauritius

Additional Stimulus Package (Miscellaneous Provisions) Act 2009

Computer Misuse and Cybercrime Act 2003

Constitution of Mauritius 1968

Criminal Code Cap 195

Data Protection Act 2004

Data Protection Regulations 2009

DNA Identification Act 2009

Electronic Transactions Act 2000

Finance (Miscellaneous Provisions) Act 2009

Information and Communication Technologies Act 2001

Interpretation and General Clauses Act 1974

Law Reform Commission Act 1992

National Computer Board Act 1988

Proclamation No. 45 of 2004

Proclamation No. 5 of 2009

Morocco

Loi n° 09-08 Relative à la Protection des Personnes Physiques à l'égard du Traitement des Données à Caractère Personnel 2009

New Zealand

Privacy Act 1993

Nigeria

Constitution of Nigeria 1999

OECD

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980

OIC

Cairo Declaration on Human Rights in Islam 1990

Charter of the Organisation of the Islamic Conference 2008

Rwanda

Loi n° 44/2001 DU 30/11/2001 Organisant les Telecommunications

SADC

Data Protection Model-Law 2012

Declaration and Treaty of SADC 1992

Senegal

Décret n° 2011-0929 du 29 juin 2011 portant nomination des membres de la Commission de protection des données à caractère personnel

Loi n° 2008-12 sur la Protection des Données à Caractère Personnel 2008

Seychelles

Data Protection Act 2003

South Africa

Bantu Building Workers Act 1951

Constitution of South Africa 1996

Constitution of the Republic of South Africa 1993

Customs and Excise Act 1964

Electronic Communications and Transactions Act 2002

Group Areas Act 1950

Industrial Coalition Act 1956

Population Registration Act 1950

Prohibition of Mixed Marriage Act 1949

Promotion of Access to Information Act 2000

Promotion of Bantu Self-Government Act 1959

Protection of Personal Information Bill 2009

Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002

Revenue Laws Amendment Act 2008

Tanzania

Broadcasting Services Act Cap.306 R.E 2002

Constitution of Tanganyika 1961

Constitution of Tanganyika 1962

Constitution of the United Republic of Tanzania 1977

Constitution of Zanzibar 1984

Constitutional Review Act 2011

Electronic and Postal Communications Act 2010

Fair Competition Act Cap. 285 R.E 2002

HIV and AIDS (Prevention and Control) Act 2008

Human DNA Regulation Act 2009

Interim Constitution of Tanzania 1965

Prevention of Terrorism Act 2002

Regulations and Identification of Persons Act 1986

Tanzania Communications Act Cap. 302 R.E 2002

Tanzania Communications Regulatory Authority Act Cap.172 R.E 2002

Tanzania Intelligence and Security Service Act 1996

Tunisia

Loi n° 2004-63 Portant sur la Protection des Données à Caractère Personnel 2004

United Kingdom

Data Protection Act 1984

Data Protection Act 1998

Human Rights Act 1998

United Nations

Declaration of Geneva: A Physician Oath 1948

Declaration of Helsinki: Ethical Principles for Research Involving Human Subjects 2000

Declaration of Helsinki: Recommendations Guiding Medical Doctors in Biomedical Research Involving Human Subjects 1964

Geneva Declaration of Principles 2003

Guidelines for the Regulation of Computerized Personal Data Files 1990

HIV/AIDS and the World of Work, ILO Code of Practice, Geneva 2001

International Covenant on Civil and Political Rights 1966

Protection of Workers' Personal Data, ILO Code of Practice, Geneva 1997

Statute of the International Court of Justice (ICJ) 1945

United Nations Convention on the Rights of the Child 1989

Universal Declaration of Human Rights 1948

United States of America

American Convention on Human Rights 1969

Cable Communications Policy Act 1984

Children's Online Privacy Act 1999

Computer Matching and Privacy Protection Act 1988

Driver's Privacy Protection Act 1994

Electronic Communications Privacy Act 1986

Fair Credit Reporting Act 1970

Family Educational Rights and Privacy Act 1974

Grammm-Leach-Billy Act 1999

Health Insurance Portability and Accountability Act 1996

Privacy Act 1974

Privacy Protection Act 1980

Right to Financial Privacy Act 1978

Safe Harbor Agreement 2000

Telecommunications Act 1996

Video Privacy Protection Act 1988

Zimbabwe

Zimbabwean Access to Information and Protection of Privacy Act Chapter 10:27

Zimbabwean Interception of Communications Act 2007

Table of Cases

Council of Europe

Campbell v United Kingdom (1993) 15 EHRR 137

Gaskin v United Kingdom, ECtHR, Strasburg, Application No. 10454/83[1989]

Malone v United Kingdom (1984) 7 EHRR 14

Pierre Herbecq and the Association Ligue des droits de l'homme v Belgium, Decision of 14 January 1998 on the applicability of the applications No. 32200/96 and 32201/96(Joined) Decisions and Reports, 1999

European Union

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) v Administración del Estado, ECJ Case C-468/10 and C-469/10

Bavarian Lager Co. Ltd v Commission, CFI Case, T-194/04

Bodil Lindqvist v Åklagarkammaren i Jönköping, ECJ Case C-101/01

Direktsia Obzhalvane i upravlenie na izpalnenieto Varna v Auto Nikolovi, ECJ Case, C-203/10

European Commission v Federal Republic of Germany, ECJ Case, C-518/07

European Parliament v Council of the European Union and Commission of the European Communities, ECJ Joined Cases, C-317/04 and 318/04

Kalliopi Nikolaou v Commission, CFI Case, T-259/03

Mauritius

Complainant v Respondent, Ref.No:-DPO/DEC/4

Complainant v Respondent, Ref.No:-DPO/DEC/5

Complainant v Respondent, Ref.No:-DPO/DEC/6

Complainant v Respondent, Ref.No:-PMO/DPO/DEC/2

Complainant v Respondents 1 and 2, Ref.No:-DPO/DEC/3

Complainant v Respondents 1 and 2, Ref.No:-DPO/DEC/7

Complainant v Respondents 1, 2, and 3, Ref.No:-PMO/DPO/DEC/1

South Africa

Bernstein v Bester NO, 1996(2) SA (A); (2) SA 751 (CC)

De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, 2004(1) SA 406(CC)

De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, 2004(1) SA 406(CC)

Financial Mail (Pty) Ltd v Sage Holdings Ltd, 1993 (2) SA 451(A)

I & J Ltd v Trawler & Line Fishing Union and Others (2003) 24 ILJ 565(LC)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty); In re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO, 2001 1 SA 545 (CC)

Jansen van Vuuren v Kruger, 1993(4) SA 842(A)

Jansen van Vuuren v Kruger, 1993(4) SA 342

Joy Mining Machinery v NUMSA and Others (2002) 4 BLL 372 (LC)

National Media Ltd v Jooste [1996] 3 SA 262(A)

NM and Others v Smith and Others, 2007(5) SA 250

O'Keeffe v Argus Printing and Publishing Co Ltd, 1954 (3) SA 244(C)

PFG Building Glass (Pty) Ltd v Chemical Engineering Pulp Paper Wood and Allied Workers Union and Others (2003) 24 ILJ 974(LC)

Protea Technology Limited and Another v Wainer and Others [1997] 3 All SA 594

S v Kidson, 1999(1) SACR 338(W)

Waste Products Utilisation (Pty) Ltd v Wilkes and Another, 2003(2) SA 515(W)

Tanzania

Attorney-General v Lesinoi Ndeinai & Joseph Selayo Laizer and Two Others [1980] T.L.R 214

Bernado Ephraim v Holaria Pastory and Gervazi Kaizilege, (PC) Civil Appeal No. 70 of 1989, HCT, Mwanza (Unreported)

Christopher Mtikila v Attorney General, Miscellaneous Cause No.10 of 2005, HCT, Dar es Salaam (Unreported)

Chumchua s/o Marwa v Officer i/c of Musoma Prison and the Attorney General, Miscellaneous Criminal Cause No. 2 of 1988, HCT, Mwanza (Unreported)

Director of Public Prosecutions v Daudi Pete [1993] TLR 22

Hatimali Adamji v East African Posts and Telecommunications Corporation [1973] T.L.R. 6

Jackson Ole Nemeteni and 19 Others v the Attorney General, Misc. Civil Cause No. 117 of 2004, HCT, Dar es Salaam (Unreported)

Julius Ishengoma Francis Ndyanabo v Attorney General, Civil Appeal No. 64 of 2001, CAT, Dar s Salaam (Unreported)

Kukutia Ole Pumbun and Another v Attorney General and Another [1993] TLR 159

Legal and Human Rights Centre and Others v Attorney General, Miscellaneous Civil Cause No. 77 of 2005, HCT, Dar es Salaam (Unreported)

Mkami Kasege & Ismail Msengi v Risasi, Conciliation Case No. 1 of 2005, 1997-2007, MCT 111

Re Innocent Mbilinyi, Deceased [1969] H.C.D 283

Sia Dominic Nyange v Mwananchi Communications Ltd, Civil Case No. 155 of 2005, the Resident Magistrate's Court of Dar es Salaam, Kisutu (Unreported)

United Kingdom

Common Services Agency v Scottish Information Commissioner [2008] UKHL 47

David Paul Johnson v the Medical Defence Union [2007] EWCA Civ 262

Michael John Durant v Financial Service Authority [2003] EWCA Civ 1746

Wainwright v Home Office [2003] UKHL 53; [2003]3WLR 1137

William Smith v Lloyd TBS Bank plc [2005] EWHC 246(Ch)

United States of America

Griswold v Connecticut, 381 U.S. 479 [1965]

1. Introduction

1.1 Background

The discourse of privacy protection has significantly evolved over years. Bennett observes that record keeping on individuals (the reason upon which data privacy laws partly emerged to regulate) is as old as civilisation itself.[1] The Roman Empire, for example, maintained an extensive system of taxation records on its subjects, who were identified through census taking.[2] Yet, the modern conception of privacy and data protection can be traced from Warren and Brandeis' seminal article 'the Right to Privacy', published in the Harvard Law Review in 1890.[3] Indeed, this article is increasingly acknowledged by commentators as the official birth date of the right to privacy in the world. However, it was in the 1960s and 70s that concrete privacy and data protection regulations emerged. This is unsurprising because the rise of computer technology around that time increased the many possibilities with which organisations, both public and private as well as individuals could process personal information in ways that could interfere with an individual's privacy.[4] This phenomenon has made Solove to remark that the small details that were once captured in dim memories of fading scraps of paper are now preserved for ever in the digital minds of computers, vast databases with fertile fields of personal data.[5] Clarke argues that the collection and collation of large amounts of personal data create many dangers to both

[1] Bennett, C. J., Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, Ithaca/London, 1992, p.18.

[2] Roos, A., 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study', LL.D Thesis, UNISA, 2003, pp.1-2. See also Roos, A., 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position', South African Law Journal (SALJ), 2007, Vol.124, No. 2, pp.400-437, at p.402. It is noteworthy that the most extreme example of census abuse is Hitler's use of the census to track minorities for extermination during the NAZI regime, see, EPIC., 'The Census and Privacy', http://epic.org/privacy/census/ last visited 3/10/2011. For more discussion about privacy risks associated with population census, see, the famous census-judgement of the German Federal Constitutional Court in 1983, Federal Constitutional Court, Judgment of 15 December 1983, no. 1 BvR 209/83.

[3] Warren, S.D and Brandeis, L.S., 'The Right to Privacy,' Harvard Law Review, 1890, Vol.4, No.5, pp.193-195; this work has frequently and traditionally been cited in numerous scholarly writings on the history of the right to privacy.

[4] It was also around the same time that academics and researchers across the world and more specifically in Europe and America started to carry out researches on the interception of law and technology including issues of privacy and data protection. For example, the Norwegian Research Centre for Computers and Law (NRCCL) was one of the first academic institutions to take up the challenge information technology posed to law and legal research. In 1970, Professor Knut S. Selmer asked the then appointed research assistant Jon Bing (now a professor) to look into the issue of "computers and law". The first result was a seminar held on 16 March 1970, which the NRCCL has qualified as its "day of birth", http://www.jus.uio.no/ifp/english/about/organization/nrccl/
last visited 3/10/2011.

[5] Solove, D.J., 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', Stanford Law Review, 2001, Vol. 53, No.6, pp. 1393-1462, at p. 1394.

individual and societal levels.[6] At an individual level, once information is in a database a data subject has significantly less control over his personal data.[7] This may in turn lead to lack of subject knowledge of data flows and blacklisting.[8] At a societal level, databases create a prevailing climate of suspicion and repressive potential for a totalitarian government.[9] Revealing the fears modern technologies have carried over individual's privacy, George Orwell, in his renowned novel *1984,*[10] portrayed the totalitarian government's ability to control its citizenry in a popular metaphor *Big Brother is watching you*. From such time onwards the *Big Brother* metaphor became an all catch phrase for state intrusion of individual's privacy.[11] Yet, despite its populism the *Big Brother* metaphor has been criticised on several grounds. Solove, for example, attacks the Orwellian metaphor for its failure to explain privacy problems resulting from computer databases. He argues that the metaphor arose in a totally different context: police search tactics, wiretapping and video surveillance, and drug testing.[12] Thus its application has been wrongly extended to privacy problems emanating from computer databases. In contrast, Schwartz[13] and Whitaker[14] have criticised the *Big Brother* metaphor for being reduced to the domain of state while excluding the private sector. As a result, they have been forced to use the term *Little Brother* to capture the use of computer database in the private sector.[15] In the same vein, Burchell argues that the powers of a *Big Brother* are no longer restricted to governments, political parties or the

---

[6] Clarke, R., 'Information Technology and Datavaillance' Communications of ACM, 1988, Vol. 31, No. 5, pp. 498-512, at pp.505-508; see also Froomkin, A. M., 'The Death of Privacy?' Stanford Law Review, 2000, Vol.52, No.5, pp. 1461-1543, at p. 1472.

[7] Froomkin, p.1464, note 6, supra.

[8] Ibid, p.1472.

[9] Clarke, p.505, note 6, supra.

[10] Orwell, G., 1984, Penguin Books, New York, 1972(Originally published in 1948).

[11] See for example, Slemrod, J., 'Taxation and Big Brother: Information, Personalisation, and Privacy in 21st Century Tax Policy', a lecture given at the Annual Lecture to the Institute of Fiscal Studies, London, September, 26, 2005, www.bus.umich.edu/otpr/WP2006-1pdf last visited 3/10/2011; Safier, S., 'Between Big Brother and the Bottom Line: Privacy in Cyberspace', Virginia Journal of Law and Technology, Spring, 2000, Vol. 5, No.6, http://www.vjolt.net/vol5/issue2/v5i2a6-Safier.html last visited 3/10/2011; Eden, J.M., 'When Big Brother Privatizes: Commercial Surveillance, the Privacy Act, 1974, and the Future of RFID', Duke Law & Technology Review, 2005, No.20, pp.1-24; Baruh, L., 'The Guilty Pleasure of Watching like Big Brother: Privacy Attitudes, Voyeurism and Reality Programs', January, 2007, a dissertation available from ProQuest, http://www.repository.upenn.edu/dissertations/AAI326087 last visited 3/10/2011. Kantarcioglu, M & Clifton, C., 'Assuring Privacy when Big Brother is Watching', DMKD03:8th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery, 2003; Ncube, C.B., 'Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-surveillance in South Africa', SCRIPTed, 2006,Vol.3, No.4, pp.344-354.

[12] Solove, p. 1397, note 5, supra.

[13] Schwartz, P.M., 'Privacy and Democracy in Cyberspace', Vanderbilt Law Review, 1999, Vol.52, pp.1609-1701, at p.1657 cited in Solove, D.J., 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', Stanford Law Review, 2001, Vol. 53, No.6, pp. 1393-1462, at p. 1397.

[14] Whitaker, R., The End of Privacy: How Total Surveillance Is Becoming a Reality, The New Press, New York, 1999, pp.160-75 cited in Solove, D.J., 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', Stanford Law Review, 2001, Vol. 53, No.6, pp. 1393-1462, at p. 1397.

[15] However in the present day environment where there is mass convergence of technology as well as close collaborations between public and private institutions, the distinction between public and private sector is almost blurred. For contrary views, see Blume, P., 'Data Protection in the Private Sector', Scandinavian Studies in Law, 2004, Vol.47, pp.297-318.

wealthy but extend to ordinary individuals.[16] Be as it may, expressions such as *Big Brother*, *Little Brother*, *Small Sisters*[17] and *databanks*, are all attempts to demonstrate the nature and magnitude of privacy problems associated with computer technology. However such problems magnified and became complex with the rise of the Internet in the 1990s. As a result, personal information can now be collected from remote computers and distributed instantly across the globe. In line with this view Zimmerman posits:-

> 'As technological innovations have become more advanced, mechanisms for monitoring people's behaviour without their knowledge have become increasingly prevalent. Indeed, "[n]ew multimedia communications and computing technology is potentially much more intrusive than traditional information technology because of its powers to collect even more kinds of information about people, even when they are not directly aware they are interacting with or being sensed by it. Not only does this new computing technology allow the collection of more data, but it also allows collectors to do more with the data they acquire.'[18]

On the Internet, user active participation or passive collection techniques provides possibilities for collection of his or her personal information. This point is well observed by commentators as follows:-

> 'When people log on the Internet and visit Web sites, a great deal of personal information is collected through both active user participation and passive collection techniques. Web sites collect information through active participation when, for example, users place online orders, fill out sweepstakes entry forms or register to gain access to "members only" sites. Conversely, the three most common forms of passive data collection methods include Web site's use of cookies, a direct marketing company's use of cookies, and an OSP's collection of "click stream" data.'[19]

---

[16] Burchell, J., 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid', Electronic Journal of Comparative Law, 2009, Vol. 13, No.1, pp.1-26, at p.1.
[17] See, Olsson, A.R., 'Big Brother, Small Sisters and Free Speech: Reanalyzing some Threats on Personal Privacy', Scandinavian Studies in Law, 2004, Vol.47, pp.373-387.
[18] Zimmerman, R.K., 'The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century', Journal of Legislation and Public Policy, 2000, Vol. 4, pp. 439-464, at p. 441.
[19] Ibid, p.442.

Cookies have great abilities. They can collect personal information and send it to data controllers without leaving behind any trace. Zimmerman generally argues:-

> 'Cookies can betray an Internet user's privacy in two primary ways. First, cookies are stored on the user's hard drive and can be accessed at a later date. Once accessed, the cookies will display a detailed list of each Web site that has been visited by the computer within a relevant time frame. Furthermore, the text of the cookie file may reveal personal information about the user, such as the user's password, e-mail address, or any other information entered while at the site...The second way in which cookies may affect privacy is that the servers on the Web sites who send cookies also receive the information stored on that particular cookie a user makes a return visit to the same site. Using cookies, Web sites currently have the ability to track from what site the user came, the links on which the user clicked while in the site, any purchases made, and any personal information entered. Many cookies are also able to identify the Internet protocol (IP) address of the user, thus giving them the capacity to identify the exact location of the computer used to access the site.'[20]

The Swedish *Bodil Lindqvist v Åklagarkammaren i Jönköping*[21] offers yet another direct illustration of the impact of technology over data collection techniques. In that case, Ms. Lindqvist was held responsible for infringement of privacy by uploading personal information of her colleagues on website some of such information contained sensitive healthy information. This made anyone in the world connected to the Internet to have access to such information. Moreover, the recent rise of social networks such as *Facebook*, *Twitter*, *MySpace*, *Hi5*, *LinkedIn*, etc has made privacy issues on the Internet much more complex.[22]

---

[20] Ibid, pp.443-444.

[21] European Court of Justice (ECJ), Case C-101/01; see also, Makulilo, A.B., 'Does the Lindqvist Decision by the ECJ make sense in terms of its treatment of the application of Art 25 of Directive 95/46/EC to uploading and downloading of personal information on internet homepages?' A Tutorial Paper presented at the Norwegian Research Centre for Computers and Law (NRCCL), Spring, 2006.

[22] For discussion about issues of privacy on social networking see, Humphreys, L *et al.*, 'How much is too much? Privacy issues on Twitter', www2.research.att.com/~bala/papers/ica10.pdf, last visited 3/10/2011; see also Barnes, S.B., 'A Privacy Paradox: Social Networking in the United States', First Monday, 2006, Vol.11, No.9, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312 last visited 3/10/2011.

As pointed out, the legal response to the rise of computer technology with respect to protection of individual's privacy had been to enact data protection legislation.[23] The point has to be made, however, that while technological factors occupied the central role to the emergence of data protection laws, there were other factors that operated as catalysts. Bygrave discusses three main catalysts for emergence of data protection laws: first, technological-organisation trends(growth in amount of data stored and their integration, increased sharing of data across organisational boundaries, growth in re-use and re-purposing of data, increased risk of data misapplication, information quality problems, and diminishing role of data subjects in decision making process affecting them), second, public fears (fears over threats to privacy and related values and restriction in transfer of personal data and thereby in goods and services), and third, legal factors (influence of international human rights instruments proclaiming rights to privacy as well as insufficiency of protection of privacy under existing rules).[24] However, in 2004, he expanded this list to include ideological factors as essential in determining privacy levels. Central amongst these are attitudes to the value of private life, attitudes to the worth of persons as individuals, and sensitivity to human beings' non-economic and emotional needs.[25] He notes that concern for privacy tends to be high in societies espousing liberal ideals.[26] Yet, in 2010, Bygrave elaborated the so called ideological factors to include cultural, religious and philosophical factors.[27] It is important to note that Bygrave added this last set of catalyst (ideological factors) for emergence of data privacy amid the growing interest by European academics and researchers to study data privacy issues in non-Western cultures. This view is supported by Bygrave's own observation:-

---

[23] The first data protection law in the world was adopted by the German *Land* of Hesse in October 1970. Then followed Sweden (1973), the United States (1974), Germany (1977), France, Denmark and Austria (1978), Luxemburg (1979), New Zealand (1982), the United Kingdom (1984), Finland (1987), Ireland, Australia, Japan and Netherlands (1988), see Roos, (LL.D Thesis) p.17, note 2, supra. Today almost all western countries have adopted data protection legislation. After the EC Data Protection Directive 1995 came into force in 1998; countries belonging under the European Union were required to implement the Directive in their national laws leading to revision of their original data privacy laws. Likewise, the Directive 95/46/EC of the European Parliament and of the Council of the 24th October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data (hereinafter the European Data Protection Directive) is currently under serious review just to take into account the technological development and societal advances that have taken place since 1995, more particularly after the internet; European Union, 'Data Protection Reforms-Frequently Asked Questions', MEMO/10/542, Brussels, November, 4, 2010,
europa.eu/rapid/press Releases Action. do? Reference= MEMO/10/542. In contrast there is a slow growth of data privacy legislation in non-Western countries. Africa is the least continent with regard to such developments.

[24] Bygrave, L. A., Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague/London/New York, 2002, Chapter 6.

[25] Bygrave, L. A., 'Privacy Protection in a Global Context – A Comparative Overview', Scandinavian Studies in Law, 2004, Vol. 47, pp. 319–348, at p.328.

[26] Ibid.

[27] Bygrave, L.A., 'Privacy and Data Protection in an International Perspective', Scandinavian Studies in Law, 2010, Vol. 56, pp.165-200, at p.175.

> 'Over the last four decades there has been an enormous growth in the field of law and policy which directly addresses privacy-related concerns, particularly with respect to the processing of personal information. While certainly not old, the field has now attained considerable maturity, spread and normative importance. It is augmented by an immense body of commentary analysing privacy issues from a variety of perspectives. Surprisingly, up-to-date comparative overviews of this development are scarce. This article is an attempt to lessen some of the gaps.'[28]

Bygrave's above view finds support of Cannataci who observes:-

> 'The debate on Privacy and Information Technology has been predominantly carried out from a "Western" perspective for over forty years. It is only relatively recently that an interest has arisen in examining whether other cultures, such as those which characterise China and Muslim societies, may stand on similar issues.'[29]

Similarly, the interest to research on privacy in non-Western cultures is amply demonstrated by Gutwirth. In his book, Privacy and the Information Age,[30] Gutwirth devotes a sub-chapter 'Privacy across Cultures'[31] to address privacy issues in other cultures and societies. It is submitted that although the computer and the Internet and concomitantly privacy concerns manifested themselves firstly in the Western world their impact has reached far. Due to globalisation, there has been a speedy penetration of these technologies to developing countries.[32] This phenomenon

---

[28] Bygrave, p.320, note 25, supra.

[29] Cannataci, J.A., 'Privacy, Technology Law and Religions across Cultures', Journal of Information, Law and Technology, 2009, Vol.1, pp. 1-22, at p.3.

[30] Gutwirth, S., Privacy and the Information Age, Lanham/Boulder/New York/Oxford/ Rowman & Littlefield Publ., 2002.

[31] Ibid, pp.24-26.

[32] See, Mayer, J., 'Globalisation, Technology Transfer and Skill Accumulation in Low-Income Countries', United Nations Conference on Trade and Development, Geneva, August, 2000; United Nations, 'Globalisation of R&D and Developing Countries', Proceedings of the Expert Meeting, Geneva, 24-26 January, 2005; see also, Wiley, J., 'The Globalisation of Technology to Developing Countries', Global Studies Student Papers, Paper No.3, http://digitalcommons.providence.edu/glbstudy_students/3 last visited 3/10/2011. Although the so called "North-South Digital Divide" is still a problem(see, Martin, B., 'The Information Society and the Digital Divide: Some North-South Comparisons', International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2005, Vol. 1, Issue 4, pp. 30-41) there are efforts to curb the problem to ensure the gap is bridged, see, Guðmundsdóttir, G.B., 'Approaching the Digital Divide in South Africa', NETREED Conference, 5-7, December, 2005, Beitostølen, Norway; Joseph, K.J., 'Transforming Digital Divide into Digital Dividend: South-South Cooperation in Information-Communication Technologies', Cooperation South, 2005, pp.102-124, http://www.rrojasdatabank.info/Joseph.pdf last visited 3/10/2011; Gupta, A., 'The Role of Knowledge Flows in Bridging North-South Technological Divides: A case analysis of biotechnology in Indian

has led scholars to use the term *global village*[33] to explain the global interconnectedness via communications. As it was the case with the West, the prevalence of computer technology in developing countries is leading to surveillance societies.[34] Africa is no exception. This surveillance has generated similar fears and concerns for individuals' control over their personal privacy as those of European counterparts.[35] In this context therefore, the objective of this study is to investigate, evaluate and analyse privacy concerns in sub-Saharan Africa along the lines defined by the research problem as well as research questions in 1.2.1 and 1.2.2 respectively.

1.2 Methodological Approach and Rationale

1.2.1 Research Problem

Most national constitutions of African countries contain express provisions for protection of the right to privacy in their Bill of Rights.[36] Yet, only Cape Verde (22 January 2001), Seychelles (24 December 2003),[37] Burkina Faso (20 April 2004), Mauritius (17 June 2004), Tunisia (27 July 2004), Senegal (15 January 2008), Morocco (18 February 2009), Benin (27 April 2009) Angola (17 June 2011), Gabon(25 September 2011) and Ghana (10 February 2012) have implemented comprehensive data privacy legislation in EU's style to give effect to such broad constitutional provisions on the right to privacy.[38] The rest of African countries have either adopted sector

---

agriculture', Centre for Science, Policy, and Outcomes, Washington, 2003; see also, Chakraborty, S., 'Mobile Phones Bridging the Information Divide Issues and Lessons from Africa', JOMC223.

[33] For detailed discussion on origins of the term 'global village' see e.g., McLuhan, M., The Gutenberg Galaxy, University of Toronto Press, 1962; Maggio, N., '"The Whole Earth as Village": A Chronotopic Analysis of Marshall McLuhan's 'Global Village' and Patrick McGoohan's The Prisoner', M.A Thesis, Brock University, Ontario, 2008.

[34] In this context the term 'surveillance society' is assigned a broader meaning to include the activities or operations of public and private organisations as well as individuals in as far as privacy violations are concerned. This is contrary to 'Big Brother' metaphor which focused on state interference of privacy while excluding the private sector.

[35] For a detailed discussion about these privacy fears and how they shaped privacy consciousness in African context, see for example chapters 4, 5, 6, and 7 of this thesis.

[36] Zimbabwe and Kenya (before 2010) have constitutions without express provisions on the right to privacy. Yet Zimbabwe is currently debating a draft new constitution with a privacy provision in its Bill of Rights.

[37] It has to be clearly pointed out that, although Seychelles has a data privacy legislation that resembles Directive, 95/46/EC in that it is also 'comprehensive' yet it significantly departs from the European law in many respects. It is arguable that since the Act extensively focuses to regulate computer bureaux's use of data and personal data, it is worth to call this law 'Computer Bureaux Act'. Further that the Act's data protection principles are limited.

[38] Commentators have given incomplete account or made factual errors with regard to the state of privacy law in Africa. This relates, first and foremost, to the countries which have implemented comprehensive data privacy laws in Africa. So far most of the pre-existing scholarly works give inconcrete list. For example, in 2002, Gutwirth failed to mention Cape Verde as an African country with data protection legislation since 2001, see Gutwirth, note 30, supra. Similarly, in 2004 Lee A. Bygrave noted that none of the African countries had implemented a comprehensive data privacy law while that was not the case, see, Bygrave, p.343, note 25, supra. Elizabeth M. Bakibinga in her article 'Managing Electronic Privacy in the Telecommunications Sub-Sector: The Ugandan Perspective', 2004, http//:thepublicvoic.org/eventscapetown04/bakibinga.doc, p.4 subscribes to Bygrave's account. In 2009, Adam Mambi, in a power point presentation, 'Internet Governance (IGF): Legal Issues on Cyber Security' Mauritius, March, 2009, listed South Africa, Mauritius and Seychelles as African countries with comprehensive data privacy

legislation by then. In 2010, Christopher Kuner in 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future', TILT Law & Technology Working Paper No. 016/2010 October 2010, Version: 1.0, p.6, Social Science Research Network Electronic Paper Collection, http://ssrn.com/abstract=1689483 noted that African countries with comprehensive data privacy law by 2010 were Benin, Burkina Faso, Mauritius, Morocco, South Africa and Tunisia. In the same year, i.e. 2010, Lee A. Bygrave noted that Burkina Faso, Tunisia, Morocco and Mauritius were the only African countries with omnibus privacy legislation, see Bygrave, p.193, note 27, supra. In 2011, Christopher Kuner in 'Table of Data Protection and Privacy Law Instruments Regulating Transborder Data Flows', Annex to the study 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future', TILT Law & Technology, Social Science Research Network Electronic Paper Collection, http://ssrn.com/abstract=1783782 listed Benin, Burkina Faso, Mauritius, Morocco, Senegal and Tunisia as countries with comprehensive data protection legislation in Africa. In the same year, David Banisar provided a list of African countries with comprehensive data protection legislation as on 1st November 2011 in a 'Data Protection Laws around the World Map', http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 last visited 20/12/2011. In that map Banisar lists Angola, Tunisia, Morocco, Senegal, Benin and Burkina Faso as African countries with comprehensive data privacy legislation. Yet, the map left out Mauritius, Seychelles and Cape Verde. In 'Information Privacy Law by Country', http://www.informationshield.com/intprivacylaws.html last visited 20/12/2011, Morocco and South Africa are listed as African countries with comprehensive data privacy legislation. Jeff Rohlmeir lists none of African countries as having data protection legislation, see 'International Data Protection Legislation Matrix', http://www.accinfosys.com/docs/International_Data_Protection_Laws.pdf, last visited 20/12/201. At least the most comprehensive list of African countries with data privacy legislation, although still with an omission of Seychelles, is comprised in the most recent publication of an Australian Professor, Graham Greenleaf, see Greenleaf, G., 'Global Data Privacy Laws: Forty Years of Acceleration', Privacy Laws & Business International Report, 2011, No. 112, pp. 11-17; republished by Privacy Laws & Business in monograph form as '76 Global Data Privacy Laws', September 2011. In a Global Table of Data Privacy Laws(as at 30 July 2011) at pp.14-16, Greenleaf lists alphabetically Angola, Benin, Burkina Faso, Cape Verde, Mauritius, Morocco, Senegal and Tunisia as African countries with data protection legislation. The table indicates correctly the years when such legislation was enacted though with some errors in relation to the Senegalese data privacy legislation. It must be admitted that Greenleaf's compilation of countries with data privacy legislation across the globe is resourceful for researchers, particularly those of comparative law. The periodic updates of this list are found on Greenleaf's web page at www2.austlii.edu.au/~graham. Through this, Greenleaf has added Seychelles in the list(see, Greenleaf, G., 'Global Data Privacy Laws: 89 Countries, and Accelerating', Privacy Laws & Business International Report, Special Supplement, 2012, No.115, also cited as Queen Mary University of London, School of Law Legal Studies Research Paper No. 98/2012, pp.1-13. The second factual error with regard to the state of data privacy law in Africa relates to chronological dates for adoption of privacy legislation. For example, Joan Ankotol in a compilation 'International Privacy and Data Protection Laws', 2008 p. 34 states that Tunisia was the first African country to enact a specific data protection law. However, Cape Verde was the firt country in the African continent to adopt the law, see, http://www.primr.org/uploadedFiles/PRIMR_Site_Home/Resource_Center/Useful_Links/International_Research/International_Privacy_Laws.pdf last visited 4/10/2011. Other sources mention Burkina Faso and Tunisia as the first African countries to implement data privacy legislation followed by Senegal, Morocco and Ghana, http://senegal.senego.com/societe-de-linformation-au-senegal-une-commission-des-donnees-personnelles-creee-par-decret/ last visited 29/10/2011. As it can be noted, this account is incorrect. There is yet another factual error that gives Francophone African countries the status of being in forefront in enacting comprehensive data privacy legislation, while in non-Francophone Africa only South Africa has a privacy bill; see, Bygrave, p.193, note 27, supra. This is also an incorrect account as Cape Verde, a former Portuguese colony appears to have data protection legislation since 2001 and Seychelles a former British colony implemented a comprehensive data privacy law in 2003 well beyond the so called Francophone Africa. It is interesting also to point that Bygrave classifies Mauritius as one among Francophone African countries; however, this is not the case although, of course, having French spoken in the country has made Mauritius to get benefits from Francophone countries. This, notwithstanding, did not apply to the enactment of the Mauritian Data Protection Act 2004(this is according to the researcher's interview with Mauritian Data Protection Commissioner -Mrs. Drudeisha Madhub on 4/07/ 2011 in Port Louis, Mauritius). It is worth noting that although French is spoken in Mauritius as it had once been under the French domination, it was the British who officially colonised Mauritius after the Berlin Conference which partitioned Africa among European powers, hence English outweighs French though they are both regarded as official languages. This is similarly the case with Rwanda, which, although it is principally a Francophone colony with French as the official language, it was admitted as a member of Commonwealth countries in 2009 which are principally Anglophone. Despite this, French outweighs English in Rwanda. Similarly, Mozambique, a Portuguese colony with Portuguese as official language, was admitted to the Commonwealth in 1995. Strictly speaking that does not make Mozambique an Anglophone country. What these incomplete accounts and factual errors tell us are two things, first, availability and access of adequate and accurate information relating to privacy in African setting is still difficult. The information available electronically is at times insufficient and out-dated to reflect the actual situation on the ground; second, the emerging scholarship in

specific legislation[39] or statutory provisions with relevancy to privacy protection in general laws.[40] Yet, in some other countries, courts have developed common law principles in resolving privacy disputes.[41] It should, however, be noted that more often one country may have a parallel approach to privacy protection.[42] Despite that-such a country may have adopted a

---

Africa is yet fluid. Mivule and Turner comment, 'there is little or no known literature on data privacy from Uganda and much of sub-Saharan Africa in general, given the relatively young and developing computing domain. At this time, to the best of our knowledge, we are the first to call for the application of data privacy techniques in Uganda' see, Mivule, K and Turner, C., 'Applying Data Privacy Techniques on Tabular Data in Uganda' http://arxiv.org/ftp/arxiv/papers/1107/1107.3784.pdf last visited 4/10/2011. From this comment, it is clear that the pre-existing literature in Africa does not seem to build upon the previous ones. There is exception with South African scholarships (e.g. Roos, 2003, 2007, 2008, see, Roos, notes 2, supra and 38 respectively) which build largely on literature from within South Africa and also from outside Africa. Outside of South Africa, few works on comparative study within Africa exist (e.g. Ncube, C.B, 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems', Journal of Information, Law and Technology, (JILT), 2004, No. 2, http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/ncube/ last visited 9/10/2011; Gayrel, C., 'Data Protection in the Arab Spring: Tunisia and Morocco', Privacy Laws & Business International Report, 2012, No.115, pp.18-20) perhaps this is also due to the little available scholarship in other African jurisdictions. The rest of the scholars (of course within the desired objectives and limitations) have limited their scope to single country analysis, e.g. Traca, J.L and Embry, B., 'An Overview of the Legal Regime for Data Protection in Cape Verde', International Data Privacy Law, 2011, Vol.1, No.4, pp.249-255; write about data protection in Cape Verde; see also Traca J.L and Embry, B., 'The Angolan Data Protection Act: First Impressions', International Data Privacy Law, International Data Privacy Law 2012, Vol.2, No.1, pp.40-45; Murungi, M.M., Cyber Law in Kenya, Kluwer Law International, the Netherlands, 2011(see chapters 6 and 8 where the author in an *ad hoc* fashion deals with privacy issues). Worthwhile to note is the fact that comparative studies on privacy and data protection laws in Africa are also lacking. As pointed out, most emerging literature has a focus in a single country. The few available comparative studies touching upon Africa have in most cases been drawing from European, American and Asia Pacific laws and practice; see for example, Roos, LL.D Thesis, note 2, supra; Roos, A., 'Personal Data Protection in New Zealand: Lessons for South Africa?' Potchefstroom Electronic Law Journal, 2008, Vol.8, No.4, pp.61-109; Mayambala, K.R., 'Phone-tapping & the Right to Privacy: A Comparison of the Right to Privacy in Communication in Uganda and Canada', BILETA, 2008; Kusamotu, A., 'Privacy Law and Technology in Nigeria: The Legal Framework will not meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/46', Information & Communications Technology Law, 2007, Vol.16, No. 2, pp. 149 – 159. While this approach is important and necessary to learn from experiences of other jurisdictions, it has at the same time undermined the growth of African scholarly writings on comparative level within the continent. Resultantly, the approach has partly caused scholars in Africa to lack information and experiences of other African jurisdictions with comprehensive data privacy laws.

[39]Most sector specific legislation regarding privacy protection in African countries cover the telecommunication sector. Some sector specific laws are comprehensive. For example, Cape Verde adopted Law No. 134/V/2001 on 22nd January, 2001 (Lei nº134/V/2001 de 22 de Janeiro) specifically to regulate processing of personal data in the telecommunications sector. This legislation is akin to the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector in terms of their scope i.e. covers the entire communication sector but not in principles they contain. In essence, Directive 2002/58/EC complements Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Note that some sector specific laws are not comprehensive in the sense that they only include few provisions with relevancy to privacy protection. See, for example, the Electronic and Postal Communications Act 2010 (Act No. 9 of 2010) in Tanzania, which although it regulates among other things, collection, storage, discloser and dissemination of personal data in the registration of SIM Cards it lacks clear principles of data processing apart from few provisions which create offences for unlawful interception and disclosure of information. See also Chapter XVI (Privacy and Data Protection, ss. 54, 55 and 56) of the Rwandese LAW N°44/2001 Governing Telecommunications, promulgated on the 30/11/2001.

[40] For instance Rwanda, Uganda, Tanzania, Ghana, Nigeria, and Cameroon have statutory provisions as well as constitutional protection of the right to privacy. This trend of parallel protection is also notable in other countries.

[41] South Africa provides a good illustration for having common law principles for protection of privacy developed over time by the courts. It is also noteworthy that apart from common law, South Africa has privacy provisions enshrined in the Constitution 1996 as well as several statutes. Further discussions see chapters 4 and 6 of this thesis.

[42] For example, Cape Verdean Constitution (Constitutional Law no. 1/VII/2010, of 3 May 2010) contains provisions for protection of privacy of correspondence (Art 44), right to demand access to correct or update one's

comprehensive data protection legislation or not. Scholars advance various explanations as to the state of privacy in Africa. These can roughly be reduced into five strands. A review of the literature comprising these strands sketches the research problem of the present thesis and consequently the formulation of research questions in the next section.

The first strand focuses on the culture of collectivism.[43] The main arguments emanating from this strand boil down to the universalism-relativism debates.[44] Gutwirth is the leading scholar in this review. In his sub-title 'Privacy across cultures', he argues that in sub-Saharan Africa privacy stands for little because of the limitation of the status of the individual.[45] He contends that due to this, the African Charter on Human and Peoples' Rights (ACHPR) 1981 fails to mention privacy even though it makes reference to the Universal Declaration of Human Rights (UDHR) 1948.The latter explicitly gives recognition to the right of privacy. He criticises the African Charter for attaching too much weight on African values and traditions which stress upon community's values at the expense of an individual's space for privacy. Gutwirth notes:-

> 'The Charter gives *peoples* a series of *collective* rights, including the right to exist, to self-determination and the right to development. Family too is propagated as the natural unit and basis of society and custodian of morals and traditional

information under public authority's control (Art.45(1)) and of being informed the purpose of collection of one's personal information(Art 45(1)). Apart from the Constitution, Cape Verde has a comprehensive data privacy legislation Lei nº 133/V/2001, de 22 de Janeiro Regime Jurídico Geral de Protecção de Dados Pessoais a Pessoas Singulares 2001 [Law No. 133/V/2001, of 22 January 2001 on protection of personal data of individuals] and above all a specific statute regulating privacy in the telecommunication sector, Law No. 134/V/2001 on 22nd January, 2001 (Lei nº134/V/2001 de 22 de Janeiro).

[43] Collectivism is defined as the theory and practice that makes some sort of group rather than the individual the fundamental unit of political, social, and economic concern. In theory, collectivists insist that the claims of groups, associations, or the state must normally supersede the claims of individuals (Stephen Grabill and Gregory M. A. Gronbacher). On the other hand individualism regards man -- every man -- as an independent, sovereign entity who possesses an inalienable right to his own life, a right derived from his nature as a rational being. Individualism holds that a civilized society, or any form of association, cooperation or peaceful co-existence among men, can be achieved only on the basis of the recognition of individual rights -- and that a group, as such, has no rights other than the individual rights of its members (Ayn Rand), http://freedomkeys.com/collectivism.htm. last visited 07/10/2011. Collectivism is likewise defined variously by different authors belonging to different disciplines.

[44] Debates on universalism and relativism manifest prominently in the human rights discourse. These doctrines are highly contested. Suffice to point out that the universalists argue that human rights are universal. They transcend all cultures. On the other hand, the relativists argue that human rights are cultural relative. The universalism-relativism debates are not settled and it is unlikely they will settle because of the diversities of people and cultures. For detailed accounts of universalism and relativism see, e.g, Shivji, I.G., The Concept of Human Rights in Africa, Dakar, Codesria, 1989, Chapter 1; Arisaka, Y., 'Beyond "East" and "West": Nishida's Universalism and Postcolonial Critique', The Review of Politics, 1997, Vol.59, No.3, pp. 541-560; Shih, C., 'Opening the Dichotomy of Universalism and Relativism', A Review of Negotiating Culture and Human Rights edited by Linda S. Bell, Andrew J. Nathan and Ilan Peleg. New York: Columbia University Press, 2001. 428 pp. and East Meets West: Human Rights and Democracy in East Asia by Daniel A. Bell. Princeton: Princeton University Press, 2000. 369 pp. Human Rights & Human Welfare, 2002, Vol.2, No.1, pp.13-24; Hellsten, S.K., 'Human Rights in Africa: From Communitarian Values to Utilitarian Practice', Human Rights Review, March-April, 2004, pp. 61-85.

[45] Gutwirth, p.24, note 30, supra.

> values recognised by the community. As a result, the group burdens the individual with duties: toward family, community, the state, the international community and other official bodies. This most likely also refers to tribes, clans, parentage, village communities and other group ties which are traditionally more important in Africa...Individualism is subordinate to the group, reducing the space for privacy.'[46]

Similarly, Gutwirth challenges the relevance of the provisions protecting privacy in constitutions of African states. He argues that even though African countries shortly after independence partly or fully adopted the legal system of their colonisers which was based on individualism, still the effect of collectivist culture rendered them ineffective in the prevailing cultural environment.[47] He stresses that in Africa informal law often takes the upper hand and people prefer the law of the village to that of the state. Gutwirth goes far to the extent of citing and subscribing to the African novelist Chinua Achebe in his *African Trilogy* who contends that solving a murder in African context is much more about finding a settlement between two tribes than a procedure to find and punish the culprit.[48] He finally makes two important conclusions: first, it is hardly imaginable that the Western concept of privacy would fit into African system, second, he considers socially and culturally Africa is a barren ground for privacy to take root and only the state and the legal system can proclaim such a thing.[49]

Gutwirth's views have parallels in Bygrave's thought too. According to Bygrave, liberal affection for privacy is amply demonstrated in the development of legal regimes for privacy protection.[50] He finds that those regimes are most comprehensive in Western liberal democracies. By contrast such regimes are under-developed in most African nations because of the collectivist cultures which place primary value on securing the interests and loyalties of the group at the expense of the individual. To substantiate his views, Bygrave observes that with exception of the African Charter on Human and People's Rights 1981 all the international and regional human rights instruments to wit, Universal Declaration of Human Rights 1948, the International Covenant on Civil and Political Rights (ICCPR) 1966, the European Convention on Human Rights and Fundamental Freedoms (ECHR) 1950 and the American Convention on Human Rights (ACHR) 1969 expressly recognise privacy as a fundamental right. He contends that the omission of

[46] Ibid.
[47] Ibid, pp.24-25.
[48] Ibid.
[49] Ibid.
[50] Bygrave, note 25, supra.

privacy in the African Charter is not repeated in all human rights catalogues even those from outside the Western, liberal democratic sphere suggesting that such omission is a result of culture of collectivism. Here he cites the example of the Cairo Declaration on Human Rights in Islam (CDHRI) 1990 which, like its Western counterparts, incorporates provision for privacy rights. Similarly, Bygrave observes that none of the African countries have enacted comprehensive data privacy laws also suggesting that individual's interests are clouded in the collectives such as family, clan, etc making privacy a less important value.[51] Nonetheless, the author singles out the Republic of South Africa as a special case where stimulus to legislate a data privacy law is provided by recent first-hand experience of mass oppression and possibly the desire to meet the adequacy requirements of the E.U Directive 95/46/EC (Articles 25-26). He notes that, the Republic of South Africa has express provision for a right to privacy in section 14 of its Constitution 1996 and Freedom of Information Act 2002. Moreover, work is underway to legislate comprehensive privacy legislation. Furthermore, Bygrave takes cognisance of the constitutional making process of a new constitution in Kenya (passed in 2010) with similar provision for privacy protection as found in the South African Constitution.

It is worth noting that Bygrave's above views first appeared in his article 'Privacy Protection in a Global Context – A Comparative Overview'[52] published in 2004. Yet, in 2010 Bygrave dramatically modified his earlier views. Undoubtedly, this shift was conditioned by the emerging data privacy laws in Africa. In his new article 'Privacy and Data Protection in an International Perspective';[53] built on 'Privacy Protection in a Global Context – A Comparative Overview', Bygrave notes that in Africa: Burkina Faso, Tunisia, Morocco and Mauritius have implemented data privacy laws. He observes:-

> 'Legal regimes for data protection are at least developed in Middle Eastern and African countries taken as a whole. As noted above, the African Charter on Human and People's Rights, 1981 omits mentioning a right to privacy in its catalogue of basic human rights. Moreover, the bulk of African countries have yet to enact European-style data protection laws. Nonetheless, some such laws have recently emerged, chiefly in francophone African states, such as Burkina Faso, Tunisia, Morocco and Mauritius...Of the non-francophone states, the

[51] Ibid, p.343.
[52] Ibid, pp.319-348.
[53] Bygrave, pp.165-200, note 27, supra.

> Republic of South Africa has come furthest along the path of establishing a comprehensive legal regime on data protection.'[54]

Bygrave advances two major reasons as to why data privacy laws start to take root in Africa. First, he attributes this development partly to the efforts made by the French Data Protection Authority (*Commission de l'Informatique et des Liberte´s* (CNIL)) to cultivate data protection in former French colonies.[55] Second, he advances economic concerns by these states, particularly the desire made by some of them to safeguard their outsourcing industries (the case with, e.g., Tunisia and Morocco).[56]

Inspired by Bygrave's earlier analyses, Bakibinga appears to argue that privacy in the African context is greatly affected by the philosophical concepts of communalism and individualism which explains the African way or approach to human rights.[57] She subscribes to Diawara's view that African philosophers emphasize communalism, collectivism and cooperation not because they are unfamiliar with individualism but because they see the value of the collective idea.[58] Bakibinga then argues that these philosophical concepts affect the evolution of societal norms that play a major role in appreciation and respect for human rights. She observes:-

> 'However individual privacy has not been fostered largely due to the subjugation of individuals' interests by communal interests. The line between what is for the individual and the community is very thin and has been reflected in society and perception of rights and obligations relating to privacy in modern times.'[59]

As Bygrave, Bakibinga says that aside the Republic of South Africa, African initiatives related to privacy have been limited. Privacy regimes are under-developed in Africa resulting in communal considerations over-riding individual and absence of legislation. Nonetheless, she argues that although in Africa the community comes first, privacy will still be an important concern as the information technology revolution advances. In this regard, she concludes, 'one can have privacy

[54] Ibid, p. 193.
[55] Ibid, p.194.
[56] Ibid.
[57] Bakibinga, pp. 2-3, note 38, supra.
[58] Ibid.
[59] Ibid, p.5.

and still be part of the community'.[60] Yet, in drawing example from Uganda, her home country, Bakibinga makes three remarks: first, that Ugandans largely suffer from 'privacy myopia' i.e. the tendency to undervalue the bits of information about themselves that it does not seem worth it to go to the trouble of protecting such information.[61] Second, aware of the existence of multiplicities of privacy definitions, she says, 'privacy has to be defined in a way that is acceptable to the Ugandan society given the emphasis on communalism versus individual rights. Privacy should not remain an abstract and one way to start would be to commission studies to obtain perceptions of privacy within the Ugandan society.'[62] Third, she recommends the adoption of privacy legislation in the EU's style.[63]

Olinger *et al*[64] offer a fairly comprehensive amount of discussion and analyses of privacy in the context of African collectivist culture. In contrast to the previous literature, Olinger *et al*, investigate privacy issues from the *Ubuntu* philosophical perspectives.[65] It is noteworthy that this investigation was carried out in South Africa at the time the South African Law Reform Commission circulated a discussion paper to solicit stakeholders' views about the forthcoming data privacy bill. The authors intended to find out to what extent, if any, the forthcoming data privacy bill in South Africa would be influenced by the EU Directive 95/46/EC on protection of personal data and the *Ubuntu* philosophy. For ease of reference the most relevant portion of this article is reproduced verbatim:-

> 'During the extensive literature review privacy was not explicitly mentioned anywhere among the *Ubuntu* writings. Privacy was glaringly absent as a cherished value or right within *Ubutntu* societies. When analysing the concepts and values of *Ubuntu* one can infer directly the implications for privacy and the attitude towards personal privacy. The statements made earlier about the welfare of the community (or group) being more important than that of the

[60] EPIC Alert, 'EPIC Hosts Privacy and Public Voice Conference in Africa', 23 December 2005, Vol. 11, No. 24, http://www.epic.org/alert/EPIC_Alert_11.24.html last visited 7/10/2011.
[61] Bakibinga, p.5, note 38, supra.
[62] Ibid, p.12.
[63] Ibid, p.13.
[64] Olinger, H.N, *et al*., 'Western privacy and/or Ubuntu? Some Critical Comments on the influences in the Forthcoming Data Privacy Bill in South Africa', the International Information & Library Review, 2007, Vol. 39, No. 1, pp. 31-43.
[65] *Ubuntu* has been defined differently by scholars (e.g. Archbishop Desmond Tutu, Louw, Mokgoro, Mbigi, etc,). However to put it in simple terms, the concept *Ubuntu* refers to African philosophy which emphasises collectivist human relationship and assistance in everyday life. In *Ubuntu*, an individual is subjected under communal considerations. The concept is well developed in South African scholarship though it has its reflection in other African societies. Find more discussions about *Ubuntu* in Chapters 4 and 6 of this thesis.

> individual immediately shows that there is a tension between privacy and social good. The case here is that personal privacy might be regarded as not being beneficial for the good of the community and in *Ubuntu* it is difficult to make the case for the social benefit of personal privacy. The culture of transparency and openness in *Ubuntu* would not understand the need for personal privacy or be able to justify it. Thus personal privacy would rather be interpreted as "secrecy". This "secrecy" would not be seen as something good because it would indirectly imply that the *Ubuntu* individual is trying to hide something-namely her personhood. The core definition of *Ubuntu*, "*people are people through other people*", indicates that there is little room for personal privacy because the person's identity is dependent on the group. The individualistic cultures of the West argue that personal privacy is required for a person to express his true individuality. With *Ubuntu* individuality is discovered and expressed together with other people and not alone in some autonomous space, and hence personal privacy plays no role in this *Ubuntu* context.'[66]

The above observations led Olinger *et al*, to conclude that the influence of *Ubuntu* would be of less significance in the development of privacy legislation in South Africa.[67] These authors advance three main reasons: first, although human dignity is the prime *Ubuntu* value that has been infused into the Constitution of South Africa, there exist no-*Ubuntu*-specific references to privacy in the Constitution neither in the current privacy related legislation in South Africa.[68] Second, although *Ubuntu* can, and has indeed influenced jurisprudence in South Africa, it could only be so in those areas where *Ubuntu* has a strong expression and philosophy.[69] In the case of privacy, *Ubuntu* leaves little doubt that privacy is not esteemed as priority for the community or for the individual. Third, the notion of *Ubuntu* is to a certain extent an idealistic concept in the world of economic realities that is regulated and controlled by international standards, rules and regulations such as those designed by, amongst others, the World Intellectual Property Organisation (WIPO) and the EU.[70] Because of that, *Ubuntu* is exclusive and limited to the African way of life. It is not incorporated into the global trade agreements and its very nature is cultural and not legal or economical. The latter make it difficult for the South African policy makers to include *Ubuntu* elements into legislation that does not translate well into international

[66] Olinger, H.N, *et al*., pp.35-36, note 64, supra.
[67] Ibid, p.40.
[68] Ibid.
[69] Ibid.
[70] Ibid.

trade of personal data. On the other hand, in finding the great influence of the EU's data privacy law to the forthcoming data privacy law in South Africa, Olinger *et al*, equally advance three reasons. First, the protection of dignity which is a core expression of the EU's data privacy law overlaps with *Ubuntu's* concept of human dignity, the South African Constitutional principle of dignity as well as the common law concept of personal dignity.[71] Second, that the South African Constitution enshrines the right to privacy as a constitutional right, which is the highest order of protection and embodiment of a right possible.[72] This is similar to the description of the privacy right in the EU's privacy legislation which is comprehensive and also compulsory to all EU member states. Third, since the EU is the major trading partner with South Africa, its directives, charters and protocols will have an influence and direct bearing on South Africa.[73] This is because of the requirement under the EU's data privacy legislation which restrict transfer of personal data to a third country unless, it has adequate privacy protection.

Critics of Olinger, *et al* such as Scorgie[74] argue that some forms of privacy: peoples' unique thoughts, ideas, characteristics and accomplishments exist in the *Ubuntu* cultures even though privacy is seen as secondary to relationships and relationship-building. People have privacy in those mentioned aspects because they fall within the private possession of an individual. Accordingly, the Western concept of privacy as dignity and part of an individual's personhood is seen to be equivalent to *Ubuntu*. Yet, comparatively privacy is less strong in the villages than in urban settings. This is what Scorgie observes, 'in rural villages in the South African province of KwaZulu Natal there is not strong sentiment towards privacy and that privacy has expressed itself as a response to community envy. Individuals that enjoy material success beyond the boundaries of the villages in urban employment become victims of community envy and tend to become "secretive" or "private" about these successes. This is a unique form of privacy that has originated to defend the individual against the community, and is by no means the norm for communitarian societies.'[75]

For completeness of this review, it is noteworthy that the *Ubuntu* philosophical perspectives in the area of privacy had been underscored before by Bakibinga and later by Burchell. However in

---

[71] Ibid, pp.40-41.
[72] Ibid, p.41.
[73] Ibid.
[74] Scorgie, F., '*Ubuntu* in Practice', HIVAN Research Associate, 2004 (Comments received by email) Email to: HN Olinger (Hanno.Olinger@Kumbaresources.com) [6 November 2004] cited in Olinger, H.N, *et al*., 'Western privacy and/or Ubuntu? Some Critical Comments on the influences in the Forthcoming Data Privacy Bill in South Africa', the International Information & Library Review, 2007, Vol.39, Issue 1, pp. 31-43, p. 36.
[75] Ibid.

both instances the discussion and analyses had been superficial. For example, Bakibinga made a brief mention of *Ubuntu* in her power point presentation by way of equating it with other African philosophies like socialism, but she did not offer an in-depth insight of the concept in relation to privacy protection.[76] In the same vein, Burchell briefly posits:-

> 'In a sense, the African concept of *Ubuntu* (we are human through others) highlights a spirit of interconnectedness or collectivity rather than individual privacy. It is the personality rights of dignity and privacy that underscore individuality and set both the limits of humanity and of human interaction. A community-centred *Ubuntu* needs to be complimented by the individualism implicit in the fundamental personality rights of dignity and privacy.'[77]

An overview of the above scholarship reveals that the first strand over-emphasises individualism not only as a permanent natural condition but also a pre-condition for privacy to develop. This is misleading. There are two fallacious assumptions the individualism-determinism paradigm rests its claims. First, Western European society was founded on individualism ever since its existence. As a result, privacy has always existed in the Western world. On the other hand African society was founded upon collectivism and has continued to be so hence lacking roots for privacy. Because of that, this literature has tended to view African society as static and unchanging ignoring profound factors such as Africa's external contacts with the outsider world, particularly Europe, through the Atlantic slave trade, colonialism, neo-colonialism and globalisation.[78] It is submitted that human society is always dynamic. It transforms across time and space. This transformation may be rapid or slow across human societies depending on varying material conditions.

Schoeman,[79] in a complete chapter 'The ascent of privacy: a historical and conceptual account', provides both a historical and conceptual account of the notion of privacy as it emerged and developed in the Western cultures. Although at the end Schoeman seems to attribute the rise of privacy to the culture of individualism, which is still problematic (see the second fallacy *infra*), he situates his analyses in wider political, economic and social contexts. In other words, Schoeman

[76] Bakibinga, E.M., 'Managing Electronic Privacy in the Telecommunications Sub-sector: The Ugandan Perspective', http://thepublicvoice.org/events/capetown04/ last visited 7/10/2011(see slide 7).
[77] Burchell, p.2, note 16, supra.
[78] These factors had profoundly impacted upon the development of African societies, their social structures, economies, politics and culture. A detailed discussion about these factors is offered in chapter 4 of this thesis.
[79] Schoeman, F.D., Privacy and Social Freedom, Cambridge University Press, USA, 1992, Chapter 7.

does not look at collectivism and individualism as natural conditions which are peculiar of a particular society irrespective of those contexts. To that end, he traces the rise of privacy partly from the Greek and largely from the Roman Civilizations to the modern days. According to Schoeman what we would treat as private the Romans found no reason whatsoever to be reserved about.[80] He illustrates this point by noting that on the tombstones of Romans, often placed along the highways, surviving relatives addressed passerby with announcements, like the announcement of a father that the girl entombed was disinherited, or that of a mother announcing that another woman poisoned the boy.[81] As a whole, Schoeman observes that the Romans generally were fond of exposing wrongdoing in public, and public censure of private conduct was ubiquitous.[82] However, although the Roman law did not in fact transgress all boundaries, there was no obligation to stay clear of any domain of life.[83] In any case, Schoeman is arguing that the limits put by the law were not occasioned by norms of privacy.[84]

As time progressed especially during the Middle Ages, things began to change. By subscribing to other scholars, Schoeman observes that during the early Middle Ages attitudes toward sex were quite different: In order for a marriage to be valid, the bride and the groom, after being disrobed by their attendants, had to be placed naked on the bridal bed together in the presence of witnesses.[85] Whereas this practice evidences the degree to which virginity and consummation were key elements in marriage practices, it also tells us how private affairs of individuals were still subjected under the social control of the community. Schoeman contends:-

> 'As political, economic, and social life became more complex, and as social functions became much more differentiated, individuals were compelled to regulate their conduct, checking their impulsive character through a process of internalisation of the principles of "correct" conduct-that is, conduct that allows one to carry out one's varied functional relationship, independent of how one is inclined. Society changed its structure in moving from a basically agrarian, socially disassociated mass of small communities to a socially integrated economic and political state. Similarly, the structure of individual consciousness changed from one of impulsive and mercurial behaviour

[80] Ibid, p.116; see also Blume, P., 'Data Protection of Law Offenders', Information, Communication and Society, 1998, Vol.1, No.4, pp.442-466, at p.443.
[81] Schoeman, note 80, supra.
[82] Ibid.
[83] Ibid, pp.116-117.
[84] Ibid.
[85] Ibid, p.118.

patterns to one of habitually internalised restraints that accommodated to the demands of the more interrelated social fabric.'[86]

In ascertaining the proper rise of individualism, Schoeman posits that the individual only emerges in certain kinds of historical circumstances, because to be an individual *is* to be aware of oneself in conflict with society's norms, internalised so as to give rise to inner conflict.[87] Accordingly, this self-awareness finds a need for private spheres and, as a result, reassigns the instinctive and less socialised parts of self to domestic and mental settings.[88] Using an illustration of the English family life, Schoeman links the idea of individualism to privacy. He notes that in the early 16th century, the English nuclear family, husband, wife and children, did *not* constitute an intimate environment in which participants focused special emotional resources on, and in turn derived special emotional meaning from, their relations with one another; and privacy in one's most important relationships, including one's relationship to oneself, was not an active form.[89] Instead, the development of intimacy and meaning in personal relations and the emergence of privacy norms are correlated with the emergence of the individual as the basic social unit replacing the kin group.[90] According to Schoeman, the conception of a person as an individual comes only when individuals ask questions about life's meanings and goals and then have the responsibility of finding answers.[91] He underlines that individuals are not just entities given naturally in their entirety, but are constructed by their own personal experiences, their associations in which they participate, and the way in which they resolve conflicts.[92] And what is meant by 'individual', Schoeman says this is not a being that is socially disengaged, but rather a person who has some say over which associations include her.[93] Other factors advanced by Schoeman regarding the emergence of the individual and consequently the notion of privacy include the Reformation, literacy, and scientific, medical and technological developments.[94]

Schoeman's views find parallels in Sihlongonyane, who in comparing the Western and African societies with regard to individualism, correctly puts:-

---

[86] Ibid, pp.118-119.
[87] Ibid, p.120.
[88] Ibid.
[89] Ibid, p.121.
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Ibid, p. 131.
[94] Ibid, pp.132-133.

> 'Questions may arise about generalisation on Western and African values and practices at this point. It probably suffice to indicate that the initial traditional standpoint of both African and Western values were similar among primitive societies. For instance, communal bonding was strong and the notion of the "nation as a family", the king and queen mother as father and mother of the nation respectively existed among other things. However, the shift from these notions has been drastic in the West than in African societies. Industrialisation, urbanisation and technological advancement have removed numerous factors that nurture the "bonding factor". From the industrialisation of the modern era (1500-1800) families started spending less time together as a unit. Husbands were stolen by the industry and women were custodians of the house. In the 20th century, even women began to be absorbed by the workplace creating a space between family members. The introduction of formal schooling further created more space between the parents and children. In the process, the social forces (i.e. religion, social rules, mores, etc) of bonding family members were undermined. Eventually, industrialisation became a way of life and the order of progress. Similarly, urbanisation further weakened the social strings in the family. Strong sentiments for individualism started gaining popularity and became more meaningful to the economic life than social life of the urban environment. Materialism and individualism eventually became synonymous with urban life, a life that economises.'[95]

In line with the above view, Walter Rodney,[96] [97]a renowned Guyanese historian, observes that before Africa came into first contacts with Europeans in the 15th Century, there were in the former uneven development of social formations. He identifies four types of these social formations: hunting bands, communalism, feudalism and societies in transition from communalism to feudalism. Nonetheless, the predominant principle of social relations was that of family and kinship associated with communalism. Undoubtedly, these social relations were reinforced by low level of productive forces which made it necessary for an individual to rely upon the labour of another in the process of material production. In this case an individual could

[95] Sihlongonyane, M.F., 'The Invisible Hand of the Family in the Underdevelopment of Africa Societies: An African Perspective', Scholarly Paper Series 1., http://www.gdrc.org/icm/country/scholarly/fanafrica.html last visited 7/10/2011.

[96] Rodney, W., How Europe Underdeveloped Africa, East African Educational Publishers, Nairobi/Kampala/Dar es Salaam, 1972, p.47.

[97] For identical views based on Marxist perspective, see Engels, F., The Origin of the Family, Private Property and the State, International Publishers Co. Inc., New York, 1942, pp.175-181.

not stand on his or her own. However with the development of productive forces man did no longer need another man in producing materials for his or her needs. Yet, the scholarship in the first strand does not address this parameter in assessing the collectiveness of individuals in the African society.

Moreover, there are noticeable self-contradictions in the defenders of individualism's account. At some point in his analyses, Bygrave cautions not to paint countries and cultures into static categories (referring to the collectivist culture in Asia and Africa which undermines existence of privacy values).[98] He justifies his caution by noting that provision for privacy rights is increasingly on the legislative agenda of some African countries.[99] Bygrave's caution became real in 2010 when he noted the existence of data privacy laws in Burkina Faso, Tunisia, Morocco and Mauritius. Paradoxically, he stresses that liberal affection for privacy is amply demonstrated in the development of legal regimes for privacy protection which are most comprehensive in Western liberal democracies. Now, if we were to argue as Bygrave that African society is collectivist as a result no genuine concept or value of privacy exists, and at the same time observe that provision for privacy rights is increasingly on the legislative agenda of some African countries, we are left in serious logical contradiction. First, Bygrave maintains a sweeping stance that African cultures are collectivist, yet he does not explain the motivations for increasing legislative agenda for provision of privacy rights in African countries. The reasons he advanced in 2010 with regard to the emerging data privacy law in Francophone African countries are in no way connected to individualism. For instance, it is difficult to comprehend how the Data Protection Authority in France *(Commission de l'Informatique et des Liberte´s*) was able 'to cultivate data protection' in Francophone African countries. Bygrave does not further explain what is meant by 'cultivating data protection'. Does this include planting individualism in such countries or it just ends with creating only capacities to enact such laws? While certainly the French Data Protection Authority could provide capacities in Francophone Africa to enact privacy legislation, it could not descend individualism in Francophone African countries as a suitable pre-condition for data privacy law to develop. Still on the first issue, it is not quite clear why despite the 'cultivation' of data protection by the French Data Protection Authority only isolated countries in the sub-region have implemented data privacy legislation while a large number of them do not have even data privacy Bills. Second, although he cautions not to paint countries and cultures in static categories suggesting that, privacy legislative agenda in Africa is a result of cultural

[98] Bygrave, p. 328, note 25, supra.
[99] Ibid.

transformation; he does not further explain whether such development is likely to result into individualism in the hitherto African collectivist culture.

Gutwirth faces the same problem as Bygrave. In assessing the Western society with regard to the development of privacy, he observes that privacy is not a given mankind has been endowed with since the dawn of time.[100] On the contrary, privacy has developed throughout history. He traces the Western notion of privacy into three main epochs: the Greco-Roman antiquity, Middle Ages and Renaissance-Enlightment.

According to Gutwirth, during Greco-Roman antiquity, privacy was seen as something negative. The individual who withdrew into private sphere (one of deprivation) was not considered better than a slave with no bearing on public life. At that time, there was no personal dignity or self-respect without public function or responsibility. The situation slightly began to change towards the end of the Greco-Roman era. Within a few centuries self-image turned into the valorisation of Christian self-constraint symbolised by the individual confession. The *homo civicus*, who could only achieve self-fulfilment by controlling the public sphere, was shoved aside by the *homo interior*, who considered self-constraint a goal in itself.

During the Middle Ages the situation became deplorable. Gutwirth observes, 'in feudal times, there was little space for privacy because of the paradoxical reason that all power was private. There was neither public debate nor public space where the common good was considered or served. Conviviality, communality and promiscuity made things individual suspect. But, as time went by, Christianity carved out a little niche for the individual: the prescribed, regular, individual and discrete practice of confession forced individuals into solitary introspection.'[101] Yet, the foundations of contemporary perception of privacy came to be created in the period between the Renaissance and Enlightenment, driven by a series of cultural political events. During this time there developed a central state which created order, reinforced its powers and control over its subjects. Family too took central stage as an important link in the pacification and maintenance of public law and order. However, the family's private domain, which used to be poor second to the fame and honour of public life, was upgraded. It is important to point that during reformation, the religious movement boosting the individual confession and introspection was also spreading, even beyond the confines of the Roman Catholic Church.

[100] Gutwirth, p.20, note 30, supra.
[101] Ibid, p.21.

Gutwirth also observes that literacy and literature expanded the potential of intellectual independence. Even if despots rule, even if the public sphere was lacking and even if *le secret du roi* still reigned, the conditions for the emergence of the individual sphere were being created. In continental Europe the development of privacy was only superficially and momentarily interrupted during the French Revolution years. Nonetheless, the French Revolution laid the foundations for a sharper legal separation between the public and private spheres.

Gutwirth's account of development of privacy in Europe runs against his conclusions about privacy developments in Africa. In sharp contrast to the above observation, Gutwirth rules out a possibility of similar notion of privacy in the West to develop in Africa. Interestingly he argues that only the state and the legal system can proclaim such a thing (i.e. privacy development). This view is against individualism explanation. Moreover, Gutwirth's conclusion is an 'ought' statement in the 'is' form thus creates controversy in the individualism-determinism paradigm.

Self-contradictions are also arising in Bakibinga's analyses about African privacy. First, while she maintains that the notion of privacy in Africa is seriously affected by the culture of collectivism she continues to argue that 'one can have privacy and still be part of the community' suggesting that within collectivism Africans may still claim privacy. Bakibinga fails to reconcile these highly contested values. Again, she calls for re-definition of privacy concept in a way that is acceptable to the Ugandan society given the emphasis on communalism versus individual rights. This call falls in the same trap. Bakibinga's recommendation for Uganda to adopt privacy legislation in the EU's style is not anywhere justified. It is arguable that if individualism is a pre-condition for privacy to develop, at least according to Bakibinga's account, then her recommendation to adopt privacy legislation in EU's style is misplacement of arguments.

The second fallacy of the individualism-determinism paradigm in the first strand is to assume that the privacy discourse arouse immediately with the rise of individualism. Critics of the individualism-determinism paradigm challenge the paradigm on three grounds. The first is the chronological problem. They argue that demand for legal protection for privacy came so very late in the day, long after the rise of individualism, whenever it actually started.[102] Perri 6 notes:-

[102] 6, P., The Future of Privacy: Private Life and Public Policy, Vol.1, DEMOS, London, 1998, p.23; Sorensen and Oyserman on individualism posits, 'the concept can be traced back to the late 1700s during the French Revolution when individualism was first used to describe the negative potential impact focusing on individual rights would have on larger societal welfare and structure', Sorensen, N. and Oyserman, D., 'Individualism', p.517, http://sitemaker.umich.edu/daphna.oyserman/files/sorensen_oyserman_2009_individualism_1_.pdf last visited 9/10/2011; see also Bezanson who argues that privacy as a concept arose in response to the industrialization, the

> 'The first legal decisions on privacy do not really appear until the very beginning of the twentieth century; the main constitutional commitments and international conventions offering some general protection are all phenomena of the second half of the twentieth century; and the main statutory interventions such as data protection legislation all appear in the last quarter of the twentieth century. Indeed, privacy has been a latecomer in the development of liberal constitutional or legislative rights for the individual and is still relatively insecurely grounded by comparison with eighteenth and nineteenth century efforts to buttress rights against arbitrary arrest, rights to freedom of conscience, association, speech and to vote for elected representatives.'[103]

Peri 6's criticisms are supported by many commentators. Bennett, for example, underscores:-

> 'By the late 1960's this development (technological determinism) had raised within post-industrial democratic states a complex but common set of fears that crucial individual rights and liberties were being compromised. States then responded with data protection statutes, designed to regulate the collection, storage, use and disclosure of recorded information relating to identifiable individuals and thus protect the value of personal privacy.'[104]

Based on the above, individualism-determinism fails to offer a clear chronological account of the rise of privacy. Second, is the geographical problem relating to individualism paradigm. The argument runs as follows: in many conventional ways (limited labour market regulation, social insurance and so on), the most individualistic society on earth is surely the United States, which has as yet no general data protection law at federal level.[105] Moreover, in the USA, individualist arguments about economic liberty are frequently deployed against proposals for data protection or press privacy law, on the grounds that these would present unacceptable interventions in

---

growth of urban areas and the impersonalisation of work and social institutions, most notably the institution of communication, Bezanson, R.P., 'The Right to Privacy Revisited: Privacy, News and Social Change 1890-1990', California Law Review, 1992, Vol.80, No.5, pp.1133-1175, at p.1137.

[103] P, p.23, note 102, supra.

[104] Bennett, p. Vii, note 1, supra.

[105] P, p. 23, note 102, supra.

freedom to trade using personal information.[106] Third, is the logical problem. The logical problem with the individualist history is that many claims to privacy cannot readily be reduced to claims of liberty and autonomy. The concerns of data protection and press privacy law are not all about the power or right to make certain fundamental or important kinds of decision for oneself and carry them out without the obstruction of government coercive power.[107] Rather, they tend more often to be about claims to *dignity*.[108] However, despite the problems of individualism determinism, Perri 6 still argues that together with urbanism and informatics, individualism gradually contributed to the rise of privacy as he notes, 'although none of these is an adequate explanation of why privacy came to be so salient so late, individualism, urbanism and informatics no doubt all play a role in the gradual rise of concern about privacy'[109]

Apart from the two fallacies discussed, there are also problems of empirical evidence supplied by the scholarships in the first strand in support of their arguments. In all cases, the literature on collectivism, as explanatory factor to the state of privacy in Africa, suffers from weak empirical evidence. To begin with, the absence of a privacy provision in the African Charter of Human and Peoples' Rights 1981 is widely cited in the discourse as evidence of lack of value to privacy. It is noteworthy that immediately after independence from colonial powers African countries adopted constitutions which incorporated the Bill of Rights.[110] Most of them included provisions on privacy.[111] Compared to the African Charter, African national constitutions came so very earlier. Moreover, they continued to exist at and after the adoption of ACHPR. Thus, if according to Bygrave, mere mention of a right to privacy in ACHPR could be an evidence of Africans' value to the right of privacy, then the inclusion of provisions on a right to privacy in African independence constitutions negates his argument out rightly. However to argue this way is probably misleading for two reasons. First, most independence constitutions in Africa were not rooted in the African soils. Instead, they were 'imposed' by their colonizers. Scholars argue that such 'imposition' did not reflect the African societal values.[112] Gutwirth, for instance, argues that although African states adopted the constitutions of their colonisers founded on

[106] Ibid.
[107] Ibid.
[108] Ibid, p.24.
[109] Ibid, p.25.
[110] Tanzania serves as an example of African countries whose independence constitutions did not contain Bill of Rights. The Tanzanian Bill of Rights came in the Constitution in 1984 through the Fifth Constitutional Amendment but was suspended until 1988 when it came into force.
[111] Kenyan Independence Constitution 1963 serves as an example of those Bills of Rights in African independence constitutions which did not contain specific provision for protection of privacy. However, the New Kenyan Constitution 2010 secures very specifically the right to privacy in Article 31; see also note 36, supra.
[112] Ugochukwu, B. E., 'Africanizing' Human Rights in Africa: Nigeria and Kenya Constitutions in Context', 2010, pp.1-38, at pp.1-4, http://ssrn.com/abstract=1691004 last visited 8/10/2011.

individualism, the collectivist culture continued to outweigh the individual's right to privacy.[113] This view is similarly echoed by Shivji who observes that most black African countries, as they marched into independence in the '60s, were bequeathed the Westminster constitutional and political order in the former British colonies, while constitutions in French-speaking Africa were modelled on analogies taken from French or Belgium.[114] Yet, all the former British colonies were given written constitutions with protection of fundamental rights as part of the independence package.[115] Shivji, just like other scholars, argues that the motive behind the inclusion of fundamental rights in the independence constitutions was to protect the property interests of the settler minority and foreign companies. [116] [117] In support of the above claim, Shivji remarks, ' this argument is buttressed by the fact that the same powers were little concerned with fundamental rights, separation of powers or independent judiciary, etc during their own rule in the colonies.'[118]

However care must be taken in generalising the use of the term 'imposition' of independence African constitutions and with respect to the Bill of Rights in particular. For instance, South Africa can be cited as an illustration of a country where the term 'imposition' must sparingly be used. This is because it is widely acknowledged that the 1996 South African Constitution was the result of several years of negotiations between dominant black, white, and Afrikaans parties.[119] Indeed its incorporation of religious and cultural rights in the Bill of Rights is evidence that it reflects the values of the majority South African people.[120] Affirming this view, Keeva states:-

> 'South Africa's constitution was negotiated by the people whose interests it must protect. In most sub-Saharan African countries, constitutions have been

[113] Gutwirth, note 47, supra.
[114] Shivji, p.18, note 44, supra.
[115] Ibid, p.19.
[116] Shivji's account is partly inaccurate for generalisation of the nature of the independence constitutions in British colonies more particularly the Bill of Rights. For example, the independence constitutions for Tanganyika (now Tanzania mainland) and Ghana had no Bill of Rights. For detailed discussion see pp. 23-25 of this thesis, Chapters 4 and 7 of this thesis.
[117] Shivji, p.19, note 44, supra.
[118] Ibid.
[119]Goodsell, E.E., 'Constitution, Custom, and Creed: Balancing Human Rights Concerns with Cultural and Religious Freedom in Today's South Africa', Brigham Young University (BYU) Journal of Public Law, 200, Vol.21, No.1, pp.109-152, at p.111.
[120] Scholars still argue that many of the rights embraced by the South African Constitution and Bill of Rights do not reflect majoritarian sentiments; instead, they are based on international human rights norms, see Johan D. van der Vyver, 'State-Sponsored Proselytization: A South African Experience', 14 EMORY INT'L L. REV. 779, 815 (2000) cited in Goodsell, E.E., 'Constitution, Custom, and Creed: Balancing Human Rights Concerns with Cultural and Religious Freedom in Today's South Africa', Brigham Young University (BYU) Journal of Public Law, 2006, Vol.21, No.1. They also argue that despite the official refusal to consult with international bodies during the drafting of the Constitution, international actors and norms had a 'subtle' and 'pervasive' influence on the values enshrined in the South African Constitution, see Heinz Klug., Constitutional Democracy: Law, Globalism and South Africa's Political Reconstruction, Cambridge University Press, 2000, p.70.

> imposed by departing colonial rulers. Those documents tended to vest power in ruling elite and ignore the particular needs of the nation. South Africa's new constitution draws on this experience and broadly embodies the nation's values because of the diversity of opinion brought to the negotiating table.'[121]

Despite that, South African courts have given considerable weight on the provisions conferring individual rights in case of conflicts with the religious and cultural rights while interpreting the provisions of the Bill of Rights in the South Africa's constitution.[122] This tells us that the inclusion of provisions reflecting African values in the Constitution, which are collective in nature, does not necessarily warrant their protection. The South African courts seem to have upheld individual rights showing that individualism is becoming more important than collectivism.

Tanganyika, a former British colony, offers another peculiar illustration where the term 'imposition' has to be cautiously used. [123] The country rejected the inclusion of the Bill of Rights in her independence constitution making use of the term 'imposition' obsolete. Martin observes that in Tanganyika a Bill of Rights was considered by the government immediately before independence and again when the constitution for the Republic was under discussion.[124] On both occasions the idea was rejected.[125] Bill of Rights was inserted in the Tanzanian constitution 23 years after independence vide the Fifth Constitutional Amendment made in 1984. It is interesting to note that all such time up to 1988 when the Bill of Rights came into force, the Tanzanian High Court rejected to enforce individual rights that were simply declared in the preamble.[126] However since 1988 the High Court and even the Court of Appeal of Tanzania (the Supreme Court) have been prepared to give force to individual rights.[127]

---

[121] Keeva, S., 'The Threat of Unrest: Traditions Provide Hope for Stability', ABA Journal, 1994, Vol.80, No.4, pp.50-60, at p.59.
[122] Ibid.
[123] In 1964 Tanganyika (which became independent of British colonial rule in 1961) united with Zanzibar to form the United Republic of Tanzania (or simply Tanzania).
[124] Martin, R., Personal Freedom and the Law in Tanzania: A Study of Socialist State Administration, Oxford University Press, Nairobi/Dar es Salaam/ Lusaka/ Addis Ababa, 1974, p.40. See also, Reed, J. S., 'Human Rights in Tanzania', in Legum, C, and Mmari, G., (eds) Mwalimu: The Influence of Nyerere, London/Dar es Salaam/Treaton: James Currey/Mkuki na Nyota/ Africa World Press, 1995, p.129.
[125] Ibid.
[126] See, Hatimali Adamji v East African Posts and Telecommunications Corporation[1973] T.L.R, 6; see also, Attorney-General v Lesinoi Ndeinai & Joseph Selayo Laizer and Two Others[1980]T.L.R 214 where in a separate judgement(note that the Court of Appeal of Tanzania is dully constituted when it is presided by three judges, except in applications and sittings of a full bench) Justice Kisanga(J.A) (as he then was) had the following to say, 'a preamble is a declaration of our belief in these rights. It is no more than just that. The rights themselves do not become enacted thereby such that they could be enforced under the Constitution. In other words, one cannot bring a complaint under the Constitution in respect of the violation of any of these rights as enumerated in the Preamble;

A case closer to Tanganyika is Cameroon. The latter, which was partly former French and British colony, has a constitution which did not incorporate a Bill of Rights at the time of independence. Instead, the Cameroonian Constitution recognized the basic rights in its preamble.[128] Chofor Che observes that the Constitution of Cameroon 1996 does not have any Bill of Rights.[129] He argues that although there is reference to political and socioeconomic rights, rights to development and peace in the preamble remain less important because such rights do not form part of the Bill of Rights.[130] In support of this view, Chenwi argues that the preamble part of the Constitution of Cameroon is unenforceable.[131] However Chenwi's argument has been made without reference to Article 65 of the Cameroonian Constitution. Akonumbo rightly posits:-

> 'Unlike the constitutions of some other African countries that clearly and extensively deal with fundamental rights under separate relevant headings (e.g. Mali, Senegal and Gabon), the Cameroon Constitution merely recalls the country's commitment to the relevant human rights instruments and specifically mentions some, such as the right to life, the right to work and the right to property. While there may be doubts and a divergence in views as to the persuasiveness and binding power of the preamble of a constitution in comparison with the constitutional provisions themselves, article 65 of the 1996 Constitution unequivocally discards such debate. This article provides that '[t]he Preamble shall be part and parcel of this Constitution'. The obvious implication is that the Preamble is no less than any part of, or provision in, the Constitution; the fundamental rights expressly or impliedly referred to in the Preamble have the same status and effect as individual provisions in the body of the Constitution.'[132]

---

see also Peter, C.M., 'The Enforcement of Fundamental Rights and Freedoms in Tanzania: Matching Theory and Practice', in P.M. Peter and I.H. Juma (eds), Fundamental Rights and Freedoms in Tanzania, Mkuki na Nyota, Dar es Salaam, 1998, pp.47-59, at p. 50.

127 See for example, Chumchua s/o Marwa v Officer i/c of Musoma Prison and the Attorney General, Miscellaneous Criminal Cause No. 2 of 1988, High Court of Tanzania, Mwanza (Unreported).

128 See, the Preamble to the Constitution of Cameroon, 1996.

129 Chofor Che, C.A., 'Challenges of Incorporating and Enforcing a Bill of Rights in the Cameroonian Constitution', Cameroon Journal on Democracy and Human Rights, 2008, Vol.2, No.1, 2008, pp. 68-72 at p.71.

130 Ibid.

131 Chenwi, L.M., 'National Human Rights Institutions: A Comparative Study of the National Commissions on Human Rights of Cameroon and South Africa', LL.M Thesis, University of Pretoria, South Africa, 2002, p.17.

132 Akonumbo, A.N., 'HIV/AIDS Law and Policy in Cameroon: Overview and Challenges,' African Human Rights Law Journal, 2006, Vol.6, No.1, pp. 85-122, at p. 94.

In case of Ghana, a former British colony, there was no inclusion of a Bill of Rights simply because provisions were not previously on offer.[133] Bill of Rights came subsequently hence it cannot be argued that such instrument was imposed at independence. It is submitted that although the Bill of Rights was less important in Africa immediately after independence, the situation significantly changed in 1980s and 1990s. The pressure that mounted from within and outside Africa culminated to inclusion of Bill of Rights in most African constitutions together with other constitutional reforms.[134] This was either through re-writing of new constitutions or effecting substantial amendments. It can be argued that as African constitutions have undergone several changes or amendments since independence warranting protection of individual's freedom and basic human rights, it would be erroneous to maintain wholly that the individual rights currently available in the African constitutions do not reflect the values of the African people.

There is another argument that runs against the view that the omission of a privacy provision in ACHPR suggests lack of value to privacy in Africa. Analogously the American constitution does not contain any express provision on the right to privacy yet the American Supreme Court has implicitly interpreted the Fourth Constitutional Amendment as protecting the right to privacy.[135] If an omission of privacy right in the American constitution does not lead to a conclusion that Americans do not value privacy why then similar omission in the African Charter is automatically inferred to a negative conclusion? Seen in that perspective, how is the conclusion for omission of privacy in ACHPR be explained in the context of inclusion of privacy provision in the African Charter on the Rights and Welfare of the Child 1990?[136]

The second piece of empirical evidence supplied by individualist school of thought is the absence of comprehensive data protection legislation in Africa. It is widely acknowledged by scholars including Bygrave himself that privacy was first conceived in America.[137] These scholars also acknowledge that Western Europe has always been picking up issues with regard to data

---

[133] Reed, note 124, supra.
[134] It is important to note that although the constitutional reforms in Africa in 1980s and 1990s were partly a result of the conditions imposed by IMF and the World Bank, scholars do not view them as 'imposed' in the same way as during independence. This is partly because most of the scholars were part and parcel of local movements that pressed for such reforms. Moreover, unlike the independence constitutions which were made and just given to the colonies, the constitutional reforms were made by local legislative bodies, constitutional conferences, etc.
[135] Gutwirth, p.26, note 30, supra.
[136] OAU, African Charter on the Rights and Welfare of the Child, 1990 OAU Doc. CAB/LEG/24.9/49 (1990) entered into force on 29 November 1999.
[137] Bygrave, pp.320-321, note 25, supra.

privacy after being debated in the United States.[138] As pointed out, to date the United States has no comprehensive data privacy legislation in the European style. Can this lack of comprehensive data privacy legislation support a claim that Americans do not value privacy? Or there is no genuine concept of privacy in the U.S? Again, in Japan, where new data privacy legislation in a European style has been adopted, scholars argue that its implementation has been difficult.[139] [140] The reason advanced in this case is the lack of attitude towards privacy. This contention dilutes the evidence of absence of data privacy law as a support of the claim under discussion. Again, how can the absence of a privacy provision in the ACHPR explain the emerging data privacy legislation in Cape Verde, Seychelles, Burkina Faso, Mauritius, Tunisia, Senegal, Morocco, Benin, Angola, Gabon and Ghana?

The third piece of empirical evidence is about frequent reference to family, groups, people and state in ACHPR. This evidence is similarly weak. First, it avoids mentioning the existence of individual rights in Articles 2 to 17 which open with reference to *every individual*... suggesting that the Charter contains also provisions on individual rights apart from those referring to collective rights. Perhaps, the argument would have been how can the two sets of rights be reconciled in actual practice? In other words, is the *law in the books* tally with the *law in action*? As pointed out, in South Africa for example, while interpreting the provisions of the Bill of Rights, courts give considerable weight on the provisions conferring individual rights whenever these come into conflicts with religious and cultural rights.[141] Second, this piece of evidence has ignored the historical and political context in which the African Charter arose-the history of Western colonial domination, struggles for independence and development. It is therefore not surprising, that, some of the provisions of the Charter reflect the culture and values of the African people as the historical past and fact for their identity but this does not necessarily mean the practices are in conformity with the Charter.

---

[138] Ibid.

[139] See generally, Nakada, M and Tamura, T., 'Japanese Conceptions of Privacy: An Intercultural Perspective', Ethics and Information Technology, 2005, Vol.7, pp.27-36; Adams, A.A *et al*., 'The Japanese Sense of Information Privacy', Al & Society, 2009, Vol.24, No.4, pp.327-341; Murata, K and Orito, Y., 'Privacy Protection in Japan: Cultural Influence on the Universal Value', Electronic Proceedings of Ethicomp, Linkoping, Sweaden, 2005; Murata, K and Orito, Y., 'Rethinking the Concept of Information Privacy: A Japanese Perspective', Electronic Proceedings of Ethicomp, Tokyo, Japan, 2007; Lawson, C., 'Japan's New Privacy Act in Context', UNSW Law Journal, 2006, Vol.29, No.2, pp.88-113.

[140] For the evolvement of privacy in China which has yet no comprehensive data protection legislation, see for example, Cheung, A.S.Y., 'China Internet going wild: Cyber-hunting versus Privacy Protection', Computer Law & Security Review, 2009, Vol.25, pp.275-279; Kong, L., ' Enacting China's Data Protection Act', International Journal of Law and Information Technology, 2010, Vol.18, No.3, pp.197-226; Yao-Huai, L., 'Privacy and Data Privacy Issues in Contemporary China', Ethics and Information Technology, 2005, Vol.7, pp.7-15.

[141] Keeva, note 121, supra.

The fourth empirical evidence is preference of the law of the village as opposed to the state. This piece of evidence is beyond the realities in Africa. Ever since Africa was put under European colonial rule in the second half of the 19th Century, there had been a constant erosion of customary law. In English colonies, for example, after the English legal system was put in place, African customary law was allowed to apply only where it was not in conflict with morality.[142]After independence, the English legal system continued to exist. This reduced significantly the domain of customary law. To date, the constitution is the supreme law in every African state (with exception of the North African Arab states where *Sharia* is the supreme law). Any law has to pass the constitutional test to be valid. Although customary law is still applicable it is insignificant. Most customary laws fail to pass the constitutional test. For example, most laws which have been denying women's rights to ownership of properties, widows' rights of inheritance, children born out of wed-lock right of inheritance, etc have been turned down as unconstitutional.[143] Gutwirth's assertion that in Africa many people prefer the law of the village as opposed to the state to the extent of settling a murder case is unsupported. It can be argued that Gutwirth's application of Achebe's *African Trilogy* to support his assertion is misdirection. This is because, the *African Trilogy* which combines Achebe's three novels (*Things Fall Apart* (1958), *No Longer at Ease* (1960) and *Arrow of God* (1964)) in one is based on the settings mostly drawn on the pre-colonial traditions of the Nigerian Igbo society as affected by colonialism. More specifically, the assertion seems to have been based upon the *Things Fall Apart* when Okonkwo, the main character, accidentally killed a boy with his gun as a result of which he was supposed according to traditions to leave his clan (Umofia) for seven years and return after expiry of such period.[144] Arguably, this was and is not the position in Africa during the colonial rule and after. It is submitted that Gutwirth contextual misapplication of Achebe's *African Trilogy* by extending 'Umofia' pre-colonial traditions in Nigeria to present day Africa is lack of understanding of the present day criminal justice in African countries.

---

[142] The question was whose morality? It definitely appears that this was the British morality. Today when customary law comes into conflict with the constitutions or statutory provisions the latter prevail to the effect that the former becomes inoperational or declared unconstitutional.

[143] See, Bernado Ephraim v Holaria Pastory and Gervazi Kaizilege, (PC) Civil Appeal No. 70 of 1989, High Court of Tanzania, Mwanza (Unreported). In that case the High Court of Tanzania nullified the Haya Customary Law which denied a woman the right to inherit under the Haya Customary Law; See also, Ozoemana, R.N., 'African Customary Law and Gender Justice in a Progressive Democracy', LL.M Thesis, Rhodes University, 2006, p. 2 who posits, 'although customary practices play a very important role in the lives of the African people as mentioned above, some of the rules can no longer withstand constitutional scrutiny.'

[144] Achebe, C., Things Fall Apart, East African Educational Publishers, Nairobi/Kampala/Dar es Salaam, 1966, pp.86-87 under licence from Heinemann Educational Books Ltd, UK.

There is also misconception in viewing South Africa and Kenya's constitutions as peculiar model in Africa by inclusion of the privacy right. This has been a problem with scholars like Bygrave[145] and Murungi.[146] Seen that way, it implies that the rest of African countries lack privacy provisions in their constitutions. This is an incorrect account. The point to be made here is that, South Africa and Kenya are the latest African countries to include express provisions for protection of privacy in their constitutions in 1996 and 2010 respectively. Moreover, this view tempts to suggest that the right to privacy embedded in the South Africa and Kenya's constitutions provides sufficient protection of privacy as such, which is not necessarily correct.

The second strand focuses on the impact of Islam over privacy. With regard to Africa, this strand is relevant to the North African Arab states (Morocco, Tunisia, Algeria, Libya and Egypt) and to some extent Nigeria (northern states) which is the only country in sub-Saharan Africa with a densely Muslim population. By and large, this strand comprises the second most contested terrain in the privacy discourse after the collectivism strand. Debates in this strand manifest in two conflicting schools of thought. To borrow Gutwirth's nomenclature, the two schools are: orthodox rejectionalist and reconciliatory.[147] The former considers human rights as part of the Western secular tradition based upon rationalism, cosmopolitanism and individualism. Islam on the other hand is a religion rooted deeply in tradition and which addresses men and women, Muslims, Christians, Jews and others differently.[148] Accordingly, an individual is viewed as part of a group and a component of a family or community structure, than as an autonomous and independent being. To make matters worse, a person must live first by Allah's commands. As a result, duties take precedence over rights and any claim for increased freedom has a touch of subversivity about it. An individual can claim limited rights within the framework of religious law. Moreover, the rejectionist theory does not accept religious norms to be tested by earthly standards.[149] In this case, divine instructions always take precedence, even over the Universal Declaration of Human Rights. The latter school of thought subscribes to human rights law (rationalism, humanism and individualism) as part of the Muslim values. It evokes an Islam which no longer badly clashes with the Universal Declaration, and which does not have to take any human rights lessons from a great many secular nations and politicians.[150] From this perspective, a multitude of fundamental rights and freedoms seem to find their origin within the

[145] Bygrave, p.343, note 25, supra; see also Bygrave, p.124, note 27, supra.
[146] Murungi, M.M., 'Kenya's New Constitution sets New Standards for Privacy and Data Protection', January, 2010, http://michaelmurungi.blogspot.com/2011/01/kenyas-new-constitution-sets-new.html last visited 11/10/2011.
[147] Gutwirth, p.27, note 30, supra.
[148] Ibid.
[149] Ibid.
[150] Ibid, p.28.

sources of Islamic law, and more specifically in the verses of the Koran, Sunna and the Hadiths of the prophet. This is certainly so if, as some Muslim argue, the sources have to be progressively interpreted.[151]

In 2007, a more detailed account of the relationship between Islam and privacy was examined in a pilot project between the value system and rule system in Islam, with data protection law as a point of departure. This project culminated in a publication of five articles in a special issue of the *Information & Communications Technology Law*, Volume 16, Issue No. 2, in 2007. A review of these articles is important for two main reasons. First, despite some limitations, they provide in-depth analyses of the relationship between Islam and privacy in a more systematic approach. Thus, the articles make significant contribution in the privacy discourse which has previously focused in the Western secular states and at least non-Islam countries outside EU. Second, being a consolidation of articles drawn from experts in Muslim and non-Muslim worlds, the special issue offers researchers a starting point for doing research from different perspectives. To begin with, Caurana and Cannataci[152] examine the impact (applicability) of the EU Directive 95/46 on protection of personal data in the North Africa and Middle Eastern states where Islamic culture or Islamic law underlines much of everyday legal practice. According to the authors, this examination was prompted by one major factor: the movement of more and more EU-based industries of their operations to North Africa and Islamic law states in order to take advantage of lower labour costs.[153] Focusing on Jordan and Tunisia, Caurana and Cannataci observe, 'it is in Jordan's interests to introduce a law on privacy.'[154] [155] This observation has been arrived at after taking into account the fact that Jordan is a signatory of various international agreements (e.g. WTO, a trade partnership agreement with EU and a joint statement on e-commerce with the United States) that are likely to assist in propagating international standards of privacy protection in domestic law. With regard to Tunisia, the authors pinpoint that it has adopted a law on data protection. However, they argue that although such law is *prima facie* word perfect *vis-à-vis* EU Directive 95/46 its implementation is possibly seriously marred by inter alia the use of personal data for police purposes, which reportedly falls far short of the EU standard entrenched in

[151] Ibid.
[152] Carauna, M.M and Cannataci, J.A., 'European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.99-124.
[153] Ibid, p.100.
[154] Ibid, p.113.
[155] As for Tunisia, the authors find that the 'core' data protection 'content' principles do find expression in the Tunisian data protection act. However they note that the extent of discretionary powers is often considerable under such law and thus the diffuse formulation of many of the law's provisions is a difficulty frequently compounded by sparse and/or nebulous commentary in the preparatory works and explanatory memoranda for the laws, see, Carauna and Cannataci, p.114, note 152, supra.

Recommendation R(87)15.[156] Unfortunately, this article does not make any analysis with respect to Islamic culture or law despite its inclusion in this special issue and its title which specifically mention the former as its units of analysis.[157]

Azmi[158] focuses her analyses in Malaysia. She observes that the Malaysian Constitution contains no specific provision on the right to privacy. The Malaysian Courts do not either recognise the right to privacy in its jurisprudence (see, *Ultra Dimension Sdn. Bhd v Kook We Kuan*). Accordingly, Azmi argues, 'in a country where individual freedom of expression is effectively not guaranteed, the European style notion that an individual should be free from unnecessary intrusion and snooping from the state is a luxury.'[159] With regard to Islam, she notes that there are some traces of privacy, nonetheless she argues, 'in a country that professes to adhere to Islamic teaching as its major religion, this proposition is entirely not acceptable.'[160] Azmi's analyses are in sharp contrast to Hayat[161] who relates privacy and Islam in Pakistan. His views are summarised as follows:-

> 'Islam recognises all human rights considered necessary for the existence, well being and personal growth of every individual in a civilized society. The human rights recognised in modern constitutions, charter and international treaties are embedded in the religion of Islam, and respect for life, privacy, freedom, equality and religious belief is an essential feature of Islam. Islam gives great importance to the fundamental human right to privacy. Islamic Shariah fully acknowledges the sanctity of one's home and private life, and there is ample admonition against prying into the affairs of others. The principles of Islam elevate the religious conscience of every Muslim, and protection of the privacy of every Muslim lies at the core of Islamic principles.'[162]

Hayat observes further that privacy is a constitutional right in Pakistan. At the same time the same constitution recognises Islam as the state religion. This means Islamic laws are supreme in

[156] Carauna and Cannataci, p.115, note 152, supra.
[157] For more discussion about privacy in various cultures, see, Cannataci, note 29, supra.
[158] Azmi, I.M., 'Personal Data Protection Law: the Malaysian Experience', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.125-135.
[159] Ibid, p.126.
[160] Ibid.
[161] Hayat, M.A., 'Privacy and Islam: From the Quran to Data Protection in Pakistan', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.137-148.
[162] Ibid, p.138.

Pakistan. By virtue of that, all laws must conform to the Holy Quran and Sunnah. To ensure this, the constitution establishes the Federal Shariat Court. The jurisdiction of this Court is to examine and decide on the question whether any law or provision of law is repugnant to the injunctions of Islam as laid down in the Holy Quran and Sunahh of the Holy Prophet. This Court can invoke its jurisdiction on a complaint brought before it or *suo motto*. Commenting on the Pakistan draft law on privacy and data protection, Hayat argues, 'there is no inconsistency with the principles and injunctions of the Quran and Sunnah of the Holy Prophet; rather this law is in accordance with fundamentals of Islam and I do not expect any problem in getting it through Parliament. Because of the power of the Federal Shariat Court, the government is always very careful in drafting and introducing laws.'[163] Hayat's analyses are problematic. They just end making a one-to-one match between aspects of privacy in Islam and the Western notion of privacy. Arguably, his approach is too simplistic. First, the author fails to differentiate between having a law on privacy and its practice. It is common knowledge that law does not operate in vacuum. Thus one would have expected Hayat to assess the Pakistan's Islamic environment and its impact on privacy instead of enumerating a long list of aspects of privacy in the Holy Quran and Sunnah. This is in sharp contrast to Azmi, who, although she finds some sorts of matching between privacy in the Holy Quran and Sunnah, she proceeds to assess the wider implication of Islamic religion on the practices of privacy rights in the Holy Quran and Sunnah. Thus, Hayat's analyses suffer from isolating the law from its context. Now, while it is easy to agree with Gutwirth on his nomenclature, which makes Hayat to fall under reconciliatory group, it is difficult to place Azmi under Orthodox rejectionist. The reason is that Azmi does not reject existence of the right to privacy in Islam rather she challenges the wider Malaysian socio-economic and political context as presently unsuitable for privacy rights to be practised.

Kusamotu[164] considers the Nigerian legal framework for protection of privacy in the context of the 'adequacy' test in the EU Directive 95/46/EC. His analyses reveal such legal framework fails to meet the standard set by the European law. Kusamotu raises three important points in connection to that: first, Nigeria does not have specific privacy laws, but guarantees the right to privacy in her Constitution; second, Article 37 of the Nigerian Constitution 1999 which secures the right to privacy is discriminatory and segregative to non-Nigerians. This provision states 'the privacy of citizen...' Accordingly, Kusamotu argues, ' it would therefore appear that in the case of the personal data of non-Nigerians that are being processed or are to undergo processing after being transferred to Nigeria, the individuals concerned will not be able to enforce their

[163] Ibid, p.145.
[164] Kusamotu, note 38, supra.

fundamental right to privacy under the Constitution;[165] third, that the absence of data protection laws in Nigeria is not connected to the percentage of Muslims in Nigeria's population or to any tenet of faith, Muslim, Christian or otherwise, but rather to the low level of data processing and awareness about its implications for privacy.[166] Arguably, the claim by Kusamotu that the state of privacy in Nigeria is explainable in the low level of data processing alone is doubtful. This is because the government, private organisations following adoption of liberalisation policies to economic, social, technological and political reforms in Africa as well as individuals, increasingly process personal data for various purposes. Moreover, it must clearly be pointed out that there are differences between processing of personal data activities and awareness of the risks that are likely to be posed by such activities on individuals' privacy. Such activities are likely to stimulate individuals' concerns for privacy. Kusamotu seems to treat the two issues in isolation. The other shortcoming of Kusamotu's arguments is that his analyses about the influence of religion on privacy, more particularly Islam, are too descriptive to support his conclusion. Moreover, in his analyses of the Nigerian legal system, Kusamotu omits discussion about Nigerian common law making such analyses incomplete.

In contrast to the previous commentators in the special issue, who specifically attempted to find the place of privacy in Islam and concomitantly its practices in Islamic states or predominantly Islamic cultures, Bonnici's analyses depart significantly from his colleagues.[167] His article focuses on discussion about relaxation of the general data protection principles in EU Directive 95/46 in the context of the EU Data Retention Directive 2006/24/EC and the proposed Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters-with its primary 'principle of availability of law

[165] Ibid, p.154; Kusamotu's views are concretised by the proposed amendments made in the News Zealand Privacy Act, 1993 in order to meet the criterion of 'adequacy' requirement imposed by Art 25 of Directive 95/46/EC to non-European countries. In a detailed report, Blair Stewart, the Assistant Commissioner in the Office of Privacy Commissioner in New Zealand, clearly stated the first recommendation by the Commissioner to be the removal of the existing requirement that in order to make an access or rectification request, an individual must be a New Zealand citizen, permanent resident, or in New Zealand at the time the request is made. According to the Commissioner, the change intended to ensure that Europeans and others have enforceable access and rectification rights, which can be exercised from outside the country, to information which is held or processed in New Zealand, see, Stewart, B., 'Proposed Amendments to NZ Privacy Act give "Adequate Protection", Privacy Law & Policy Reporter, 2001, Vol.5, http://www.austlii.edu.au/au/journals/PLPR/2001/5.html last visited 1/11/2011; see also Article 29 Data Protection Working Party, 'Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000', 5095/00/EN, WP 40, p. 5, (adopted on 26th January 2001), where the Article 29 Working Party observes that section 41(4) of the Australian Privacy Amendment (Private Sector) Act 2000 accords rights of correction to Australian citizens and the permanent residents only making EU citizens that are no permanent residents in Australia but whose data was transferred from the EU to Australia fail to exercise access and correction rights in relation to their data.

[166] Kusamotu, p.157, note 165, supra.

[167] Bonnici, J.P.M., 'Recent European union Developments on Data Protection...in the Name of Islam or "Combating Terrorism"', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.161-175.

enforcement information.' Bonnici's main contention is that the two developments in the EU law (the Third Pillar) which regulates issues of public security, defence, State security and activities of the State in areas of criminal law, all of them exempted from the general application of EU Directive 95/46, has tended to relax (or devaluate) the standards set by the latter. The main standard referred is the 'purpose specification principle' which is cardinal before any processing of personal data takes place. He argues that in the EU Data Retention Directive 2006/24/EC and the proposed Council Framework Decision, it is less clear to identify the specific purpose for processing personal data. Moreover, he contends that the broad justification for such processing i.e. counter-terrorism, which most invariably the West links it with Islam, whether by using direct terminologies such as Islamic fundamentalism, Islamic extremist, etc or indirect terminologies such as criminals, terrorist, etc in order to avoid open criticisms and confrontations from Islamic communities is extremely confusing. It is submitted that while Bonnici's analyses are relevant they address a totally different subject from the present study. As pointed out, this thesis is premised in the context of implementation of general data privacy laws. It has links to the EU Directive 95/46/EC which appears to be the main stimulus for countries outside Europe to enact data privacy laws in response to the requirements of Articles 25-26 requiring 'adequate' level of protection of personal data to be ensured in third countries when data originating from Europe to such third countries is initiated.

The third strand in the above review of literature concerns about developmentalism. Shortly after independence in 1960s and 70s, African countries, in a bid to rebuild their countries, devoted much effort to economic developments. Accordingly, other aspects of development, more specifically human rights issues, were given less priority affecting the right to privacy. Ncube takes the lead to introduce developmentalism factors in the African privacy discourse. In a review of Zimbabwean and South African data protection systems, she argues, '...from the time of independence Zimbabweans have been predominantly concerned with those rights pertaining to pressing political and economic issues such as the rising cost of living. Subsequently issues such as data protection have largely been overlooked.'[168] This is despite the fact that Zimbabwe's Independence Constitution 1980 contained a Bill of Rights albeit without an explicit provision for privacy protection. The case is different in countries such as Tanganyika where an inclusion of a Bill of Rights in the independence constitution was completely rejected by the TANU nationalists led by the late Mwalimu Julius K. Nyerere. They argued that such a Bill would

[168] Ncube, p.10, note 38, supra.

hamper the new government in its endeavours to develop the country.[169] Moreover, it would be used by the judiciary (mainly dominated by English judges) to frustrate the government by declaring most of its actions unconstitutional.[170] This rejection of the Bill of Rights persisted even after independence. The rejection is reflected in the report of the commission charged with mandate to collect opinion and views from people regarding the issue. A portion of this report states:-

> 'Tanganyika has dynamic plans for economic development. These cannot be implemented without revolutionary changes in the social structure. In considering the Bill of Rights in this context we have had in mind the bitter conflict which arose in the United States between the President and the Supreme Court as a result of radical measures enacted by the Roosevelt Administration to deal with the economic depression in the 1930s. Decisions concerning the extent to which individual rights must give way to wider considerations of social progress are not properly judicial decisions. They are political decisions best taken by political leaders responsible to the electorate.'[171]

The developmentalist camp leaves many questions to be desired. First, they wrongly view privacy as an antithesis of development. Paradoxically the very reason they advance as an excuse for overlooking privacy issues, i.e. national building is the same reason they advance for the adoption of data privacy protection legislation, i.e. economic outsourcing. Ncube observes:-

> 'Data protection is a very important international trade issue and the lack of adequate data protection may be a barrier to trade. ...The need to establish and enforce effective data protection systems in both Zimbabwe and South Africa is a trade and development issue. The 1995 European Union Data Protection Directive (http://www.bfd.bund.de/europa/EU_richtl_en.html>) imposes a standard of protection on any country in which the personal data of European citizens is processed. Such data can only be processed in countries that can guarantee adequate levels of protection (Articles 25-6)'[172]

---

[169] Martin, pp.40-41, note 124, supra; see also, Reed, note 124, supra.
[170] Martin, p.41, note 124, supra.
[171] Ibid.
[172] Ncube, p. 2, note 38, supra.

She argues:-

> 'Developing nations, especially those in Africa, as evidenced by their recent establishment of NEPAD, intend to be full participants in the global economy. Such participation will only be enabled by conducive trade relations. Zimbabwe and South Africa, like all other developing nations therefore need to ensure that their data protection laws encourage rather that(sic) discourage international trade by providing adequate levels of data protection to enable the flow of data from European Union(EU) countries.'[173]

In her other article, 'Watching the watcher: recent developments in privacy regulation and cyber-surveillance in South Africa', Ncube stresses the need to adopt privacy legislation in South Africa for economic outsourcing.[174] Other scholars who emphasise the need to adopt privacy legislation in the EU's style include Roos, Bakibinga, Kusamotu, Neethling, Murungi,[175] etc. Although none of these scholars have provided empirical evidence to show to what extent African countries have been affected by not adopting data privacy legislation in conformity with the EU's law, emphasis has been placed on developmentalism as a justification for adopting data privacy legislation. Second, African countries have continued to remain poor with or without the adoption of privacy law or Bill of Rights. Thus explaining the state of privacy in Africa on 'overlooking to address privacy issues for economic development reasons' is not well convincing.

The fourth strand of literature explains the undeveloped state of privacy in Africa simply on people's ignorance of this right. This is by far the most neglected strand. Bakibinga attributes the low level of privacy in Uganda due to Ugandans' ignorance of their right to privacy.[176] She uses Froomkin's terminology 'privacy myopia' to capture this state of affair.[177] This view is also echoed by Kusamotu with regard to privacy protection in Nigeria. He argues that the absence of data protection laws in Nigeria is not connected to the percentage of Muslims in Nigeria's population or to any tenet of faith, Muslim, Christian or otherwise, but rather to the low level of data processing and awareness about its implications for privacy.[178] While lack of awareness of

[173] Ibid.
[174] Ncube, p.346, note 11, supra.
[175] Murungi, note 146, supra.
[176] Bakibinga, note 61, supra.
[177] Ibid.
[178] Kusamotu, note 166, supra.

privacy right may partly explain the state of privacy in Africa, there is no study so far which has been carried to establish such claims.

The fifth strand comprises debates on the ability of common law to secure individuals' privacy. Two main conflicting schools of thought are noticeable within this strand. The first school largely propounded by a Nigerian professor Nwauche can well be summarised in the following paragraph:-

> 'I am of the firm opinion that a comprehensive protection of information privacy can be achieved through a tort of privacy that protects against intrusion well as disclosure as discussed above. In this way the dignity of the individual will be well protected. A tort of privacy is important as it assists the development of a constitutional right to privacy...'[179]

However Nwauche admits that there is currently little Nigerian jurisprudence over protection of privacy under the tort of breach of confidence. As a result, he is forced to rely on the English case law in his analyses which he asserts it is not clear whether such case law is binding or not on Nigerian courts. He observes that in England there is no overarching cause of action for privacy. However, various aspects of privacy protection are fast developing especially with the enactment of the Human Rights Act 1998 as a measure to incorporate the European Convention on Human Rights into English law. Perhaps because of this, Nwauche considers the protection of privacy in Nigeria through a common law tort of privacy while paying due regards to the constitutional protection of the right to privacy under Article 37 of the Nigerian Constitution 1999 which state, 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.' Unfortunately, Nwauche does not make any discussion, let alone any reference to the Directive, 95/46/EC. It is less clear whether the omission to discuss the implication of the Directive which is implemented in England, is attributable to lack of knowledge of existence of such law or otherwise. Opponents of this view and more particularly Kusamotu argues that Nigerian legal framework for privacy fails to meet the test of adequacy under the Directive 95/46/EC. Echoing this position are scholars such Chukwuyere[180] and Nwankwo[181] [182] whose discussions and analyses are largely

[179] Nwauche, E.S., 'The Right to Privacy in Nigeria', Review of Nigerian Law and Practice, 2007, Vol.1, No.1, pp.62-90, at p. 83.
[180] Izuogu, C.E., 'Data Protection and Other Implications in the Ongoing SIM Card Registration Process', 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665, last visited 11/10/2011; see also Izuogu, C.E.,

focused on the adoption of the registration of SIM card scheme in Nigeria without having appropriate data privacy legislation.[183] Further discussions with regard to sufficiency or otherwise of the common law are pounded by Bakibinga,[184]Ncube[185], Neethling [186] and Roos.[187] For example, Roos argues, that though there is rich development of the common law in South Africa with regard to privacy, the same is still insufficient. She therefore calls for adoption of a comprehensive data privacy law in the EU's style. However, critics of Roos, particularly Burchell,[188] argue that South African common law is adequate and goes far to invite Scotland to follow the South African approach with regard to protection of privacy through the tort of privacy.[189] These conflicting arguments from commentators with regard to the ability of common law to protect privacy partly explain why African states in sub-Sahara do not adopt privacy legislation. However, a thorough examination of common law with regard to privacy protection needs to be undertaken.

1.2.2 Research Questions

An overview of the above strands of literature sketches the coverage and limitations of the existing literature about protection of an individual's right to privacy in an African context. It is imperative to note that such strands are pivoted on generalised normative assumptions: cultural relativism, economic developmentalism, nature of the legal system, and to a very marginal extent lack of understanding of privacy issues. In bridging the gap left by the above strands, the present study addresses following set of questions:-

a) Does a well-defined concept or value to privacy exist in sub-Saharan Africa?

'Nigeria: Data Protection & Privacy Issues in NCC's Directive on SIM Card Registration', 2010, http://www.facebook.com/note.php?note_id=388277770826 last visited 11/10/2011.

[181] Nwanko, I.S., 'Part I: Nigeria's SIM Card Registration Regulations 2010: The Implications of unguarded Personal Data Collection', http://www.facebook.com/note.php?note_id=10150095718055827 last visited 11/10/2011.

[182] Nwanko, I.S., 'Part II: Nigeria's SIM Card Registration Regulations 2010: The Implications of unguarded Personal Data Collection', http://www.facebook.com/note.php?note_id=10150095718055827 last visited 11/10/2011.

[183] See also, Akinsuyi, F.F., 'Data Protection Legislation for Nigeria, The Time is Now!', Nigerian Muse, http://www.nigerianmuse.com/20071004075550zg/sections/general-articles/data-protection-legislation-for-nigeria-the-time-is-now/ last visited 11/10/2011.

[184] Bakibinga, p. 9, note 38, supra.

[185] Ncube, pp.3-4, 11-13, note 38, supra.

[186] Neethling, J *et al.*, Neethling-Potgieter-Visser Law of Delict, 6th Edition, LexisNexis, Durban, 2010; Neethling, J *et al.*, Neethling's Law of Personality, 2nd Edition, LexisNexis, Durban, 2005.

[187] Roos, p. 718, (LL.D Thesis), note 2, supra.

[188] Burchell, note 77, supra.

[189] Ibid, pp.25-26.

b) To what extent is privacy protected in sub-Saharan Africa? Do such means of protection reflect the pre-existing values of privacy in the sub-continent?

c) Is the emerging regime of data privacy law in sub-Saharan Africa which most invariably is styled in European Data Protection Directive 95/46/EC, a mere compliance to meet the 'adequacy' standard set by such law for non-European countries rather than a genuine attempt to ensure respect to individuals' privacy in sub-Saharan Africa?

1.2.3 Scope and Case Studies

1.2.3.1 Scope

Privacy problems are cross-jurisdictional. Concomitantly there are difficulties for a single country to address such problems in isolation from others. Yet, a collective approach to privacy problems has also been challenged. Raab posits, 'the privacy of personal information has been under threat in recent years from many quarters. Information, like money and water, flows across jurisdictional boundaries; dangers and risks are imported and exported without, as yet, the consistent ability of regulators-singly or in concert-to counter them effectively.'[190] Nevertheless, there is still merit in the collective approach hence drawing experience on other nations, how they have implemented privacy regulation, becomes imperative. In support of this view, Bygrave argues that as data-processing operations increasingly extend across national boundaries, the way in which they are to be regulated should not occur without consideration of the way in which they are regulated in a wide variety of countries, such consideration being one precondition for achieving harmonised regulation.[191] Consistent with this view, Bennett posits, 'as more and more countries passed these laws (i.e. data protection laws) they continue to draw lessons from pioneers about what worked, and what did not. Supervisory authorities learned from one another.'[192] Africa has 54 states, including the recently independent state of the Republic of

[190] Raab, C.D., 'Information Privacy: Networks of Regulation at the Sub-global Level', Global Policy, 2010, Vol.1, No.3, pp. 291-302, at p.291. Yet in an earlier article Bennett, C.J and Raab, C.D., 'The Governance of Global Issues: Protecting Privacy in Personal Information', A Paper presented in the European Consortium for Political Research, March 28- April 2, 2003, p.6, http://courses.essex.ac.uk/lw/lw656/2007/RaabBennett.pdf last visited 11/10/2011 appear to preach harmonisation of data privacy regulations through bilateral and multilateral mutual agreements.
[191] Bygrave, p.12, note 24, supra.
[192] Bennett, C.J., 'International Privacy Standards: A Continuing Convergence' http://www.colinbennett.ca/Recent%20publications/PrivacyLawand%20BusinessJune2010.pdf, last visited 11/10/2011.

South Sudan.[193] However, this research is limited to sub-Saharan Africa.[194] The North African region (Algeria, Egypt, Libya, Morocco and Tunisia) is excluded from the the present research.[195] The decision to include sub-Saharan Africa and excluding North Africa has been arrived based on the following considerations. First, despite the diversity of its people, socio-economic, and political dynamics, the sub-Saharan African countries have more shared common features than with its counterpart North African countries. Central to this is about culture. The *Bantu* culture is predominant in sub-Saharan Africa.[196] In contrast, the North African region is predominated by strong Arab and Islamic culture. As a result, the influence of such culture in the affairs of the state is very significant. For example, *Sharia* law, which is restrictive of freedom of individuals' affairs, is influential to the running of the affairs of the state and people's lives in this region.[197]

---

193 South Sudan became an independent state from Sudan on 9th July, 2011. It became a member of the African Union on 28th July, 2011 and United Nations on 14th July, 2011, see, http://en.wikipedia.org/wiki/South_Sudan last visited 28/09/2011.

194 Sub-Saharan Africa is a geographical term used to describe the area of the African continent which lies south of the Sahara or those African countries which are fully or partially located south of the Sahara, see, hhtp://en.wikipedia.org/wiki/Sub-Sahara_Africa, last visited 1/10/2011. To be precise, sub-Saharan Africa include the following countries: Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo (Brazzaville),Congo DRC (Zaire),Cote d'Ivoire, Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea- Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritania, Mauritius, Mozambique, Namibia, Niger, Nigeria, Reunion, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Swaziland, Tanzania, Togo, Uganda, Zambia, and Zimbabwe.

195 North Africa or Northern Africa is the northernmost region of the African continent, linked by the Sahara to sub-Saharan Africa. Geopolitically, the United Nations definition of Northern Africa includes eight countries or territories: Algeria, Egypt, Libya, Morocco, South Sudan, Sudan, Tunisia and Western Sahara, http://en.wikipedia.org/wiki/North_Africa, last visited 1/10/2011. In contrast the African Development Group classifies six countries as comprising the North Africa: Algeria, Egypt, Libya, Mauritania, Morocco and Tunisia, see, www.afdb.org/en/countries/north-Africa last visited 1/10/2011. Yet in further contrast, the North Africa has traditionally been defined as the region north of the Sahara comprising five countries of Algeria, Egypt, Libya, Morocco and Tunisia, see for example, International Federation of Red Cross and Red Crescent Societies, Mid-Year Report, North Africa Appeal No.MAA82001, 15 August, 2011, www.ifrc.org/docs/appeals/annual11/MAA8200111myr.pdf, last visited 1/10/2011. A similar definition of the North African region can be found at Looklex Encyclopaedia, i-cias.com/e.o/north_africa.htm. It is this last definition of the North African region which is adopted in this study.

196 For more about the Bantu cultures see, Van der Veen, L.J, *et al.*, 'Language, Culture and Genes in Bantu: a Multidisciplinary Approach of the Bantu-Speaking Populations of Africa', OMLL-01_JA27:01-B07/01-S08/01-Vo1, http://www.ddl.ish-lyon.cnrs.fr/fulltext/Van%20Der%20Veen/Van%20der%20Veen_%E0%20para%EEtre.pdf, last visited 1/10/2011.

197 Some Muslim scholars argue that Islam and specifically *Sharia* law is compatible with principles of human rights enshrined in various international and regional instruments as such they tend to regard the West as the resultant cause of misdirection: see for example discussions of 30/04/2010 between Emran Qureshi and Heba Raouf Ezzat on a topic 'Are *Sharia* Laws and Human Rights Compatible?' ISLAM 21, International Forum for Islamic Dialogue(IFID), http://www.ifidonline.com/m2/index.php/islam-21-monitor/cat_view/34-islam-21 last visited 27/04/2011; see also Mohamed Talbi who argues, 'From the Qur'anic perspective...human rights are rooted in human nature. And this is by virtue of God's plan and creation. Now it goes without saying that the cornerstone of all human rights is religious liberty, for religion, which is 'the explanation of the meaning of life and how to live accordingly', is the most fundamental and comprehensive of human institutions'; Talbi, M., 'Religious Liberty as Divine Gift', ISLAMI 21 Monitor, 2010, Issue 52-53, p.3, http://www.ifidonline.com/m2/index.php/islam-21-monitor/cat_view/34-islam-21 last visited 27/04/2011. For a detailed discussion of the jurisprudence of individual freedom in Islam see, Ahmad, N., 'A Study of Individual Freedom and Religious Liberalism in Islamic Jurisprudence', the Journal Jurisprudence, 2009, pp.41-66,

Arguably privacy right is severely limited by such cultures. Thus, it has been considered that a more specific research study needs to be carried out in North Africa taking into account these extra *Bantu* cultural peculiarities. Second, although the initial proposal of this study was to research privacy across Africa including both regions, i.e. sub-Saharan Africa and North Africa, the Arab spring which sweept the North African states in 2011 complicated the research environment.[198] First and foremost, there were security concerns. In a state of turmoil in which citizens are pressing for regime change through demonstrations, wars, etc, it was considered that the sub-region was not safe for carrying out field research. Moreover, the relationship between a researcher and interviewees, which is apparently based on trust, becomes seriously affected in an unstable and unsecured political situation. As a result, gaining access to individuals, government institutions and office bearers for research clearance, interviews or collection of documents becomes extremely difficult. Narrating his experience in a similar situation as a PhD student at Humboldt-University in Berlin, Salmon[199] states:-

> 'I landed at Khartoum airport on December 20th 2002 with few contacts and little beyond a house line up....One of these (few contacts), a pro-government Sudanese expat, used his connections to arrange passes and interviews that would have been difficult if not impossible to procure alone. These strategies slowly bore fruits, but only after almost one and a half months filled with dead end interviews, no-shows and trying to establish trust with highly sceptical interviewees.'

Salmon continues to observe, 'having arrived in Northern Sudan I discovered that not only were the National Records Office, newspaper achieves and various libraries difficult to access, but also

---

http://www.jurisprudence.com.au/juris5/nehaluddin.pdf last visited 27/04/2011. However this position has been sharply criticised by other scholars mostly Western who view Islam and particularly *Sharia* law as in conflict with principles of human rights. See for example McCrea, R., 'Limitations on Religion in Liberal Democratic Polity: Christianity and Islam in the Public Order of the European Union', LSE Law, Society and Economy, Working papers 18/2007, London School of Economics and Political Science: Law Department, www.lse.ac.ac.uk/collections/law/wps/wps.htm and Social Science Research Network library, http://ssrn.com/abstract=1033332, last visited 27/04/2011.

198 The Arab Spring (Arabic: الربيع العربي; also known as the Arabic Rebellions or the Arab Revolutions) is a revolutionary wave of demonstrations and protests occurring in the Arab world. Since 18 December 2010 there have been revolutions in Tunisia and Egypt; a civil war in Libya resulting in the fall of its regime; civil uprisings in Bahrain, Syria, and Yemen; major protests in Israel, Algeria, Iraq, Jordan, Morocco, and Oman, and minor protests in Kuwait, Lebanon, Mauritania, Saudi Arabia, Sudan, and Western Sahara. Clashes at the borders of Israel in May 2011 have also been inspired by the regional Arab Spring; see http://en.wikipedia.org/wiki/Arab_Spring last visited 29/09/2011.

199 See, Salmon, J., 'Field Research in Sensitive Areas', Junior Research Group, 'Micropolitics of Armed Groups', Working Papers Micropolitics No. 1/2006, p.9. http://www.ipw.ovgu.de/inipw_media/schlichte/mikropolitik/MicropoliticsSalmon.pdf last visited 28/09/2011.

the Bank of Sudan's economic report had been 'tidied', and the University of Khartoum(UoK) had been cordoned off after a series of anti-regime demonstrations.'[200] These hurdles presented by the Sudanese case in this example alerted the researcher to reconsider the inclusion of North Africa in the present study. However, it must be clearly mentioned that in contrast to the present study Salmon's thesis was typically a research project intended to be carried out in armed conflict regions. Because of this, he invoked a special methodology usually employed in areas of armed conflicts. It is submitted that such methodology would still present difficulties in the present study. This is because most invariably research on privacy touches many things of one's personal life. In a state of armed-conflicts, interviewees are highly suspicious about questions probing their personal lives.

However, despite being excluded from the scope of this study, where necessary reference has been made to North Africa with regard to privacy and data protection systems. The intention for such reference was not to make a detailed examination of such systems in the sub-region but rather to make contrast and sometimes comparing generally such systems with trends of privacy legislation in sub-Saharan Africa. Another reason for making such reference is the fact that North Africa is still part of Africa. Because of that, any measure, that is likely to be taken by the African Union (AU) to protect privacy, is going to affect North Africa (except Morocco) as these countries are also members of AU.

1.2.3.2 Case Studies

In order to gain in-depth insights of privacy issues in sub-Saharan Africa, Mauritius, South Africa and Tanzania were purposively selected from the rest of the countries in the sub-region. In this selection, three clusters of countries were made. The criteria used to determine a country' respective cluster was whether at the time of field research (June-September 2011) such a country had comprehensive data privacy legislation or a Bill on such law or had neither data privacy legislation nor a Bill. However, new enactments after this period but before finalisation of this study have been updated. To further clarify these criteria, countries which at one time adopted Bills on data privacy legislation and later abandoned them were classified in a cluster without data privacy legislation or Bills on such law unless such Bills were later re-introduced. This is because, first, a withdrawn Bill loses the force of being considered a Bill in the strict sense of the term. Moreover, where a Bill was yet to be introduced to parliament but subsequently

[200] Ibid, p. 12.

abandoned because of strong criticisms from stakeholders and general public opinion or the abandonment was made by government *suo moto*, such situation was similarly grouped in a cluster of countries without data privacy legislation or draft Bills. At the same time, countries with Freedom of Information Act (FOIA) were put in the cluster of countries without data privacy legislation or draft Bills. This is because, although most invariably FOIA contains special provisions regulating personal data, it falls short of data protection principles.[201] Moreover, data protection principles in FOIA have limited application. First, they apply only the moment a request for access of information is initiated; second, in most cases the legislation is only binding on the public sector. There are exceptions with regard to the second limitation. The direct case at point is South African Promotion of Access to Information Act (PAIA).[202] This Act applies to (a) a record of a public body; and (b) a record of a private body, regardless of when the record came into existence.[203] [204] It is argued that PAIA is an unusual character of FOIA across the world whose normal application is limited to the public sector.[205] It is worth noting that the emerging freedom of information law in Africa is influenced by PAIA by extending its scope to private sector.[206] However, notwithstanding the broader scope of PAIA in bringing the private

---

[201] See for example, 'Data Protection and Freedom of Information in the Public Sector', Notice No. 23 of 31 December, 2006 prepared jointly by the Irish FOI Central Policy Unit of the Department of Finance in consultation with the Office of the Data Protection Commissioner and the Office of Information Commission, issued by the Irish Office of Information Commission, http://foi.gov.ie/Data-Protection-and-Freedom-of-Information-in-the-Public-Sector, last visited 1/10/2011. This Notice attempts to interpret S. 1(5) of the Irish Data Protection Act, 1988 and S.7 (7) of the Freedom of Information Act, 1997 with regard to an individual's right of access to information held by the public sector; see also generally Turle, M., 'Freedom of Information and Data Protection-A Conflict or Reconciliation', Computer Law and Security Report, 2007, Vol. 23, pp.514-522; see also, UK House of Commons, '*The Freedom of Information Bill*: Data Protection Issues, Bill 5 of 1999-2000', Research Paper 99/99 of 3 December 1999, pp.11-16, http://www.parliament.uk/documents/commons/lib/research/rp99/rp99-099.pdf, last visited 1/10/2011; Banisar, D., 'The Right to Information and Privacy: Balancing Rights and Managing Conflicts', Working Paper, The International Bank of Reconstruction and Development/The World Bank, 2011. In the context of the South African legislation on freedom of information in relation to data protection, see, Currie, I and Klaaren, J., Commentary on the Promotion of Access to Information Act, *Siber* Ink, South Africa, 2002, p.18, para, 2.5; Roos, A., 'Data Protection' in Dana, M., *et al*, Information and Communications Technology Law, LexisNexis, Durban, 2008,pp.313-397, at p.360.

[202] Act No. 2 of 2000.

[203] Ibid, S. 3(a) & (b).

[204] Presently only seven countries in Africa have implemented Freedom of Information Act. Included in this list are South Africa(2000), Zimbabwe(2002), Angola(2002), Uganda(2005), Ethiopia(2008), Liberia(2010), and Nigeria(2011). Counties with pending Bills on FOIA include Mozambique, Kenya, Ghana, Rwanda, Malawi, Botswana, Madagascar and Sudan. Zambia had at one time introduced the Bill on FOIA in parliament but withdrew it in 2002. Tanzania had taken sometime to discuss the Bill among stakeholders but the same is yet to be introduced in parliament.

[205] See, EPIC and Privacy International, Privacy and Human Rights(2005), p.632 cited in Roos, A., 'Data Protection' in Dana, M., *et al*, Information and Communications Technology Law, LexisNexis, Durban, 2008, pp.358-359.

[206] See for example, the Liberian Freedom of Information Act, 2010, SS. 1.4(a) & (d) which extends its application to both the public and private sector. However in slight contrast with PAIA which applies to the private sector generally, the Liberian law applies to the private sector with some limitations: where private entities receive public resources and benefits, engage in public functions, and or provide public services, particularly in respect of information relating to the public resources, benefits, functions or services. S. 2 of the Mozambican Access to Official Sources of Information Bill 2005 extends the scope of application of such proposed law to the private sector whenever private entities hold informative material of public interest; see also, S.25 (2) of the Kenyan

sector under its ambit, which in absolute terms makes it at equal level with most data protection legislation, the scope of the principles in PAIA are restrictive.[207] Zimbabwe is among the earliest African states to enact FOIA. In contrast to PAIA, the Zimbabwean Access to Information and Protection of Privacy Act (AIPPA)[208]regulates only the public sector.

From the above backdrop, *cluster one* comprises countries with comprehensive data privacy legislation: Cape Verde, Seychelles, Burkina Faso, Mauritius, Tunisia, Senegal, Morocco, Benin, Angola, and Gabon. Ghana was not included in the list simply because at the time of field research she had no comprehensive data privacy legislation. She only adopted the Act after the field research. It is imperative to note that Tunisia and Morocco belong to the North African sub-region while the rest in this cluster belong to sub-Saharan Africa. *Cluster two* comprises countries with Bills or drafts on data privacy protection. In this cluster there is Ghana (which has passed its Bill into Act in February 2012), Ivory Coast (Cote d'Ivoire), Kenya, Madagascar, Mali, Niger, Nigeria and South Africa. *Cluster three* comprises countries with neither data privacy legislation nor Bills. These include Botswana, Burundi, Cameroon, Central African Republic, Chad, Comoros, Congo (Brazzaville),Congo DRC (Zaire), Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gambia, Guinea, Guinea- Bissau, Lesotho, Liberia, Malawi, Mauritania, Mozambique, Namibia, Reunion, Rwanda, Sao Tome and Principe, Somalia, South Sudan, Sudan, Swaziland, Tanzania, Togo, Uganda, Zambia, and Zimbabwe. It is important to note that in 2005/2006 Tanzania prepared a draft on freedom of information with a chapter on data protection. This draft was later abandoned from circulation and discussion before it was introduced to the parliament. Ghana presents a similar case to Tanzania. On 29 November 2010 the Ghanaian government introduced the Data Protection Bill to the parliament. However this Bill was subsequently withdrawn in July 2011. It was re-introduced to the parliament in October 2011. On 10 February 2012 it was passed into law.

To narrow down these clusters, Mauritius was selected from *cluster one*; South Africa from *cluster two* and Tanzania from *cluster three*. As pointed out, these country cases were purposively selected. A number of considerations were taken into account for these selections. To start with, the choice of Mauritius from *cluster one* was informed by the fact that the country's data protection law and practices are more transparent and accessible. Nearly all the information about Mauritian

---

Freedom of Information Bill, 2007 which subjects the private sector holding or controlling information that is necessary for the enforcement or protection of any right to the application of the proposed law.

[207] Roos, p. 360, note 201, supra.

[208] Chapter 10:27 of the Laws of Zimbabwe came into operation on 15th March, 2002 through G.N No.116 of 2002.

Data Protection Act 2004 and its enforcement is available at the Data Protection Office's website.[209] In contrast, the accessibility of similar information in the rest of the countries in *cluster one* is hardly lacking. For example, the only useful and accessible information to the researcher from Cape Verde was the data privacy legislation[210] and a more recently published article on the Cape Verdean data privacy system.[211] As to the rest of the countries, the primary information available and accessible to the researcher in Seychelles, Burkina Faso, Senegal, Benin, Angola and Gabon was only the data protection legislation in the respective countries.[212] [213] The accessibility to such information was also hampered by language constraints notably French for Burkina Faso, Senegal, Benin and Gabon and Portuguese for Cape Verde and Angola.[214] This is with the exception of Seychelles which is an English speaking country. Since the researcher is conversant in English language, Mauritius whose one of the official language is English provided a more convenient research environment. Also, compared to the rest of countries in the cluster, Mauritius has relatively sufficient level of data protection practices. For example, although Cape Verde appears as the leading African country to enact data privacy legislation, it has not yet established the data protection authority.[215] Seychelles' Data Protect Act status was contradictory. For instance, the Seychelles Legal Information Institute (SEYLII), whose mission is to provide online free public access to legal information from Seychelles, placed on its website only the

[209] See, Data Protection Act 2004 for Mauritius via http://www.gov.mu/portal/sites/ncbnew/files/DPA.pdf last visited 11/10/2011.

[210] Lei nº 133/V/2001, de 22 de Janeiro Regime Jurídico Geral de Protecção de Dados Pessoais a Pessoas Singulares 2001[Law No. 133/V/2001, of 22 January 2001 on protection of personal data of individuals], http://portoncv.gov.cv/dhub/porton.por_global.open_file?p_doc_id=407, last visited 29/10/2011.

[211] Traca and Embry, note 38, supra. This article, written in English language, provides a broader overview of the entire Cape Verdean legal system of data privacy protection.

[212] Seychelles, Data Protection Act No.9 of 2003, http://dev.seylii.org/sc/legislation/act/2003/9 last visited 11/10/2011; Burkina Faso, Loi n° 010-2004/AN Portant Protection des Données à Caractère Personnel 2004 [Act 10-2004/AN on Protection of Personal Data], www.cil.bf/legislations/loi_cil_burkina_faso.pdf last visited 29/10/2011; Senegal, Loi n° 2008-12 sur la Protection des Données à Caractère Personnel 2008 [Law No. 2008-12 on the Protection of Personal Data], http://right2info.org/resources/publications/loi_sur_les_donnees_a_caractere_personnel.pdf last visited 29/10/2011; Benin, Loi n° 2009-09 du Mai 2009 Portant Protection des Données à Caractère Personnel 2009[Law No. 2009-09 on the Protection of Personal Data in the Republic of Benin], http://ddata.over-blog.com/1/35/48/78/Benin-2/Loi-2009-protection-donnees-a-caractere-personnel.pdf last visited 29/10/2011; Angola, Lei nº 22/11 Da Protecçao de Dados Pessoais 2011 [Law 22/11 on Personal Data Protection]. Recently Traca and Embry, note 38, supra, have published an article in English about Angolan data protection legislation; Gabon, Loi n°001/2011 Relative à la Protection des Données à Caractère Personnel 2011[Act No. 001/2011 on the Protection of Personal Data].

[213] This was also the case with respect to availability and accessibility of information from Tunisia and Morocco. The former's data privacy legislation is (Tunisia) Loi n° 2004-63 Portant sur la Protection des Données à Caractère Personnel 2004 [Organic Act n°2004-63 on Protection of Personal Data], http://www.inpdp.nat.tn/version-anglaise/texte.html while the latter's similar piece of legislation is (Morocco) Loi n° 09-08 Relative à la Protection des Personnes Physiques à l'égard du Traitement des Données à Caractère Personnel 2009[Law No. 09-08 on the protection of individuals with regard to processing of personal data].

[214] Note also that the language barrier was considered in excluding Tunisia and Morocco and North Africa generally whose languages are both French and Arab.

[215] Traca and Embry, p.249, note 38, supra.

name of the Data Protection Act with a 'Not in Force' status.[216] In contrast the editorial notice on SEYLII's website under which the Data Protection Act was listed reads, 'Seychelles Acts in Force as at 20 June, 2011'.[217] However against it there was an NIF defined as Not in Force. The researcher proceeded to the field research with this status in mind. However after the field research was over, he requested SEYLII to be supplied with an electronic document of the Act, by using the 'contact us' function on the website. The link to the Act was promptly supplied on 3 October 2011.[218] This was exactly the date when the Act was uploaded on the website under 'recent posts'[219] with an 'in force yes' status.[220] [221] To ascertain the date when the Act came into force, the researcher sent a follow up email to SEYLII which was never replied. As it can be noted from this account, at the time of the field research, it was clear to the researcher that Seychelles' Data Protection Act was inoperational. The data protection authorities in Burkina Faso, Senegal and Benin were recently established hence the law was insufficiently put into practice as compared to Mauritius.[222] As for Angola and Gabon, the data protection authorities are yet to be established.[223] As pointed out, Ghana was not at all considered bedacsue she had no data protection legislation at the time of field research. There were also considerations of local research contacts established prior to the commencement of the field research. The contacts for Mauritius were obtained easily from the Data Protection Office's website. It is interesting to note that request to undertake field research in Mauritius made to the Mauritian Data Protection

---

216 SEYLII, http://dev.seylii.org/sc/table/legislation/seychelles-acts-force-20-june-2011 last visited 11/10/2011.

217 Ibid.

218Email communication from Thelma Casquette sent via telly74@gmail.com to alex.makulilo@gmail.com providing the link to the requested information to http://www.seylii.org/sc/legislation/act/2003/9.

219 See the link to the updates at SEYLII, http://dev.seylii.org/sc/legislation/act/2003/9 last visited 11/10/2011.

220 It is noteworthy that on 11/10/2011 when the researcher last visited the SEYLII's website the post relating to the Data Protection Act 2003 was only seven (7) days and twenty one hours old; see http://dev.seylii.org/tracker.

221 It is important to bear in mind that under the 'Terms of Use' on its website, SEYLII brings to the general public a disclaimer notice on the inaccuracy, incomprehensiveness or lack of up-to-date information on the Acts posted. The researcher paid attention to this disclaimer in following up the status of data privacy legislation in Seychelles.

222 For example, for Burkina Faso la Commission de l'informatique et des libertés (CIL) was established on 18 May 2007 vide Décret n° 2007-283/PRES/PM/MPDH du 18 mai 2007 portant organisation et fonctionnement de la Commission de l'informatique et des libertés [Decree No. 2007-283/PRES/PM/MPDH of May 18, 2007 on the organization and functioning of the Commission on Informatics and Liberties] http://www.cil.bf/, see also, http://www.cai.gouv.qc.ca/CCPDF/doc/bf.pdf last visited 29/10/2011. It must be pointed out that although the Office of Mauritian Data Protection Commission was proclaimed on 27/12/2004, the first Commissioner, was appointed on 10/10/2008, see http://www.gov.mu/portal/goc/mcsa/files/president.pdf last visited 29/10/2011; for Senegal, the Data Protection Commission was established on 29/06/2011 vide Decree No. 2011-0929 appointing the members of the Commission for the protection of personal data i.e Décret n° 2011-0929 du 29 juin 2011 portant nomination des membres de la Commission de protection des données à caractère personnel, http://www.demarches.gouv.sn/textes/decret_creation_cdp-2.pdf last visited 29/10/2011; surprisingly the date for establishment of the Senegalese Data Protection Commission is erroneously referred to as 20/04/2009 by Association Francophone Des Autorités De Protection Des Donnees Personnelles. This is the association for data protection authorities in Francophone, suggesting that it would be more informed on this development within its members, see, democratie.francophonie.org/IMG/pdf/Telechargez_ce_document-4.pdf last visited 29/10/2011; for Benin the Office of Data Protection Commission was established on 11 March 2010 see http://www.journal-adjinakou-benin.info/?id=4&cat=6&id2=1475&jour=12&mois=3&an=2010 last visited 30/10/2011.

223 Note that the Angolan Data Protection Law 22/11 was enacted when the researcher was in the field research, i.e. 17/06/2011. Thus in any case it would have been less fruitful to choose Angola as a case study under *cluster one.*

Commissioner (Mrs. Drudeisha Madhub) on 26 January 2011 was responded positively and quickly on the same day. Moreover in contrast to the rest of countries in *cluster one*, Mauritius has gone far to formally seek EU's 'adequacy' accreditation. Although other countries have applied for the EU 'adequacy' rating or about to do so in future, Mauritius is far in the accreditation process. These considerations made Mauritius to be selected a case country study from *cluster one*.

South Africa was selected from *cluster two*. Closely to Mauritius, the South African legislative process of the Protection of Personal Information Bill (B9-2009) which is still pending is open. All preparatory works for this Bill are accessible online from the South African Law Reform Commission's website (//www.justice.gov.za/salrc/). This made the researcher able to track the legislative process of the South African data privacy Bill since 2006, long before the formal commencement of this study. There was also a consideration of established local research contacts, in this case Professor Iain Currie and Professor Anneliese Roos, since 2006 and 2008 respectively. As we shall see, these were instrumental during field research in South Africa. Moreover, South Africa is a multi-cultural society. It was considered that this peculiar feature of South Africa should be studied to discover how such multi-culturalism operated in favour or against the adoption and operation of a data privacy law. Connected to this but in contrast to the other countries in *cluster two*, the legislative process of a data privacy law in South Africa has taken more than a decade with serious discussions and considerations. This legislative process needed to be examined in order to understand competing interests in the process. It is important to underline that in the event the South African Protection of Personal Information Bill (B9-2009) is passed into law before the finalisation of this study, the analyses for this country case will be principally limited up to the stage such Bill is passed into law but before it is put into operation. There are two important reasons for this delimitation: first, the issues that this thesis investigates will largely remain unaffected by voting such Bill into law, second, it will require sometime before the actual operation and practice of the law can be studied.

Tanzania was selected from *cluster three*. Three main considerations were taken into account for its inclusion as one of the country cases. First, it is imperative to note that Tanzania is one of the sub-Sahara African countries that practiced *Ujamaa* for a long time. Since *Ujamaa* is an ideology that is indispensable for collectivism it was considered that its development and likely impact on privacy issues be closely investigated. Second, considered for selection of Tanzania was the fact that the researcher had already undertaken two studies that culminated to the publication of two

journal articles: one relating to employees' healthy privacy[224] and the other privacy of individuals in the communication sector.[225] These prior studies had made the researcher more familiar with the country's legal system regarding privacy issues as well as the actual privacy practices. Commentators like Lipset argue, "'a person who only knows one country knows no countries" because it is only by looking across different societies that one can understand what is either typical or unique about one's own.'[226] Aware of this pitfall, comparing Tanzania with other jurisdictions became imperative. Third, Tanzania is the researcher's homeland. Standing on this advantage, the selection of Tanzania minimised to a great extent field research costs that would have been incurred by the researcher had he chosen a foreign country.

However excluded from considerations for choosing the scope and selection of case studies of this thesis were two factors. First, this research study was principally funded by the DAAD. It is DAAD's sponsorship policy that funds to Africa are only granted to researchers from countries in sub-Saharan Africa. Nevertheless, the policy does not restrict or control the nature and scope of research projects undertaken by researchers. Concomitantly, the limitation of this study to sub-Saharan African is by no means a reflection of the DAAD's policy. Second, the choice of the geographical limit and ultimately the case studies did not take into account the classifications of African countries into their respective legal systems i.e. civil and common law. This is because, while legal systems have different traditions in many respects, in terms of privacy issues, they are similar. It is important to mention that despite the specific limitation of this study to the above case studies, reference in this work has been frequently made to the rest of countries in sub-Saharan Africa as this is the overall geographical scope of this research study.

[224] Makulilo, A.B., 'You must take medical test: Do Employers intrude into Prospective Employees' Privacy?' Datenschutz und Datensicherheit (DuD), 8/2010, pp.571-575.
[225] Makulilo, A.B., 'Registration of SIM Cards in Tanzania: A Critical Evaluation of the Electronic and Postal Communications Act, 2010', Computer and Telecommunications Law Review (CTLR), 2011, Vol. 17, No. 2, pp.48-54.
[226] See Francis Fukuyama's remarks on Symour Martin Lipset(1922-2006), Journal of Democracy, 2007, Vol. 18, No. 2, pp.185-188, at p. 188; also referred in Makulilo, A.B., 'State-Party and Democracy: Tanzania and Zambia in Comparative Perspective', PhD Thesis, University of Leipzig , 2010, p. 178. See also, Lipset, S.M., 'Pacific Divide: American Exceptionalism-Japanese Uniqueness', International Journal of Public Opinion Research, 1993, Vol.5, No. 2, pp.121-166, at p.121.

1.2.4 Methods

Methods are the tools-the instruments, techniques and procedures - by which a science gathers and analyzes information.[227] Like tools in other domains, different methods can do different things.[228] Each method should be regarded as offering potential opportunities not available by other means, but also as having inherent limitations.[229] Because of the inherent pitfalls in these methods, this study employed a qualitative hybrid research approach. By hybrid it simply means a combined or mixed research approach: doctrinal and non-doctrinal. To be precise, the methodologies simultaneously involved in this study are doctrinal, empirical and international comparative law. The last two categories fall under non-doctrinal.

1.2.4.1 Doctrinal Research

This is traditionally the sole methodology of legal research. It primarily focuses on what the law is, i.e. *de lege lata* as opposed to what the law ought to be, i.e. *de lege ferenda.* Under doctrinal methodology a researcher's main goal is to locate, collect the law (legislation or case law) and apply it to a specific set of material facts in view of resolving a legal problem. This is because the major assumption of doctrinal research is that the character of legal scholarship is derived from law itself.[230] With this limitation, it is imperative to note that beyond an existing legal rule, doctrinal methodology is incapable of being used for legal analysis. To recapitulate, the main agenda of the present research is law reform. The research questions stated in 1.2.2 of this study have been formulated towards that broad agenda. In this context therefore, doctrinal research has limited application to the present study. The method is only applicable where interpretation of existing laws or at least a Bill is required. To be sure, the second research question identified in 1.2.2 requires to be approached by doctrinal research methodology. Similarly doctrinal research is used in evaluating statutory and case law in specific national jurisdictions referred in this study.

---

[227] Mcgrath, J.E., 'Methodology Matters: Doing Research in the Behavioural and Social Sciences', in R. M. Baecker *et al.*, (eds), Readings in Human-Computer Interaction: Toward the Year 2000, Morgan Kaufmann Publishers, 1995, p. 154.
[228] Ibid.
[229] Ibid.
[230] Chui, W.H and McConville, M (eds)., Research Methods for Law, Edinburgh University Press, 2010, p.4

1.2.4.2 Empirical Legal Research

Owing to limitations of the doctrinal exposition described in 1.2.4.1 and in order to overcome them, the present research engaged empirical legal research (sometimes known loosely as non-doctrinal or socio-legal or interdisciplinary research) as a supplement.[231] This mixed approach is tandem to what academic lawyers such as Baldwin and Davis argue, 'it is important to note that empirical legal scholarship is complementary to doctrinal research and both methodologies can be used simultaneously to examine legal issues.[232] [233]As to what makes research empirical, Epstein and King state:-

> '...is that it is based on observations of the world, in other words, data, which is just a term for facts about the world. These facts may be historical or contemporary, or based on legislation or case law, the results of interviews or surveys, or the outcomes of secondary archival research or primary data collection. Data can be precise or vague, relatively certain or uncertain, directly observed or indirect proxies, and they can be anthropological, interpretive, sociological, economic, legal, political, biological, physical, or natural. As long as the facts have something to do with the world, they are data, and as long as research involves data that is observed or desired, it is empirical.'[234]

Since non-doctrinal legal research uses empirical data, it provides vital insights into the law in context, i.e. how the law works in the real world.[235] In other words, non-doctrinal research deals

---

[231] In considering further limitations of doctrinal research, Siems poses a question, 'Why do we need other disciplines in order to answer these specific or general questions? Why is it not enough to do traditional legal research, in particular doctrinal research?' He then answers himself, 'The main reason is that traditional methods are often regarded as useful but too narrow. For instance, doctrinarism has been accused of being "rigid, dogmatic, formalistic and close-minded; of encouraging "intellectual tunnel-vision" through an unhealthy preoccupation with technicalities; of placing "an intellectual strait-jacket" and of impoverish[ing] the questioning spirit of both law student and teacher', See, Siems, M.M., 'The Taxonomy of Interdisciplinary Legal Research: Finding the Way out of the Desert', Journal of Commonwealth Law and Legal Education, 2009, Vol.7, No.1, pp.5-17, at p. 6.

[232] Baldwin, J and Davis, G., 'Empirical Research in Law' in P.Cane and M. Tushnet (eds), The Oxford Handbook of Legal Studies, Oxford University Press, 2003, p.881 cited in Chui, W.H and McConville, M (eds)., Research Methods for Law, Edinburgh University Press, 2010, p.6.

[233] For more discussion about advantages and disadvantages of using empirical methodologies in legal research see, Burns, K and Hutchinson, T., The Impact of "Empirical Facts" on Legal Scholarship and Legal Research Training', the Law Teacher, 2009, Vol.43, No.2, pp.166-168.

[234] Epstein, L and King, G., 'Empirical Research and the Goals of Legal Scholarship: The Rules of Inference' University of Chicago Law Review, 2002, Vol.69, No.1, pp.1-133, at pp.2-3 cited in Dobinson, I and Johns, F., 'Qualitative Legal Research' in W.H Chui and M. McConville (eds)., Research Methods for Law, Edinburgh University Press, 2010, p.18.

[235] See e.g., Razak, A.A., 'Understanding Legal Research', p.21, Department of Management and Marketing Faculty of Economics and Management, University Putra Malaysia, http://econ.upm.edu.my/researchbulletin/artikel/Vol%204%20March%202009/19-24%20Adilah.pdf,

with the externalities affecting the operation of law. As a result, empirical legal research is valuable in revealing and explaining the practices and procedures of legal, regulatory, redress and dispute resolution systems and the impact of legal phenomena on a range of social institutions, business and citizens.[236] As noted, this research has a law reformist agenda. Because of this, it was imperative that empirical research be invoked.

Sources of data for this research were mainly documents and interviews. Documents constituted the largest source while interviews were supplementary. Concomitantly, the collection, review and analysis of documents such as legislation, Bills, case law, decisions of quasi-judicial bodies, policies, hansards, reports, treaties and conventions, *travaux préparatoires*, journal articles, commentaries, reference books, newspapers, and magazines was central to the methodology of this study. However due to limitations affecting the currency, accessibility as well as reliability of some documents, a decision was made to engage unrepresentative, non-random sampling interviews to a limited scale. It must be underlined that while interviews were not the main source of data to the present thesis they were important and useful in supplementing the documentary source.

In order to gain access to documentary source, libraries, bookstores and Internet sources were highly used. The researcher's membership to the State and University Library Bremen (*Staats- und Universitätsbibliothek Bremen*) was vital to access data for this study. Moreover, being a member of freelance researchers' team to the Law, Science Technology & Society Studies (LSTS) at the Vrije Universiteit Brussel since 2009, the researcher has had access to this University library and more importantly its online resources. The researcher had also access to the University of Derby's Digital Library. This library by far provided links to numerous databases such as Westlaw, Lexis Library (formerly known as LexisNexis), HeinOnline, Wiley Online Library, Taylor and Francis, SpringerLink journal collection, and SciVerse ScienceDirect. The researcher also accessed freely the African Journals Online, AJOL, (http://www.ajol.info/).[237] The main goal of AJOL is to promote access to African research. This database helped a great deal in conducting literature review on privacy issues in African context. In South Africa, the researcher purchased temporary membership to the University of South Africa's (UNISA) Library from 28 June 2011 to 29 June 2011. He was similarly able to access freely online materials from UNISA Institutional

last visited 25/09/2011.

[236] Ibid.

[237] The African Journals Online (AJOL) is the world's largest and pre-eminent of peer-reviewed, African-published scholarly journals. AJOL is a Non-Profit Organisation based in South Africa, see, http://www.ajol.info/). Most articles in AJOL are freely accessible and downloadable in pdf. format.

Repository via uir.unisa.ac.za. Apart from access to UNISA Library, the researcher purchased books and journal articles covering privacy and human rights issues from the University of Pretoria Bookstore. Important texts purchased there include Neethling's Law of Personality, Second Edition; Neethling-Potgieter-Visser Law of Delict, Sixth Edition; Information and Communications Technology Law (Dana van der Merwe, *et al*); The Law of Delict in South Africa (Max Loubser and Rob Midgley (eds)) and the Rise and Fall of Apartheid (David Welsh). It deserves mention that the researcher received free of charge the Commentary on Promotion of Access to Information Act from one of its co-authors, Professor Iain Currie when he visited him for interview at the University of Witwatersrand (WITS). He equally received journal articles from Professor Anneliese Roos at UNISA. Moreover, in South Africa, the researcher gained free access to the South African Law Reform Commission's website (//www.justice.gov.za/salrc/) where he was able to retrieve the Issue Paper, Discussion Paper and Report on Privacy and Data Protection in South Africa. These documents were the basis of preparation of the Protection of Personal Information Bill (B9-2009). To keep abreast with the discussions and deliberations on this Bill, the researcher requested and was granted free subscription to the South African Parliamentary Monitoring Group's (PMG) website (http://www.pmg.org.za/). PGM has been monitoring South African Parliamentary Committees since 1996 to date. With such access, the researcher was able to follow closely all the proceedings and deliberations of the Parliamentary Portfolio Committee on Justice and Constitutional Development with regard to the Protection of Personal Information Bill after it was introduced in the South African Parliament on 25 August 2009.

The researcher obtained most information in Mauritius from the Data Protection Office at its current office located on the 4th Floor, Emmanuel Anquetil Building, along Corner Sir Virgil Naz & Sir William Newton Streets, in Port Louis. Many resources were also accessed from the Data Protection Office's website. Such resources are freely accessible to anybody; anywhere, provided one has Internet connection. They include for example, the Data Protection Act, 2004, its amendments and all regulations made under it. Other important documents are industry codes of good practices, comprehensive list of data controllers, decisions of the Data Protection Commissioner over complaints lodged in her office, various forms to be used in lodging complaints, registering data controllers, etc as well as numerous presentations made by the Data Protection Commissioner to various public and private sector organisations over the operation of the Act. While in Mauritius, the researcher also gained access to the Supreme Court of

Mauritius Library with the aid of his research clearance. He was also given a free subscription to the Court's online library. With such access, various legal materials were retrieved.

Similarly, the researcher gained access to various documents from the Tanzania Communication Regulatory Authority (TCRA). He also accessed freely TCRA's website (http://www.tcra.go.tz/) and retrieved legislation, regulations, reports, notices to the general public, etc. Apart from that, the researcher gained access to the Law Reform Commission of Tanzania's website (http://www.lrct.go.tz/). With its limitation of materials to the present thesis, the researcher was able to retrieve only a Position Paper on Electronic Commerce law which very remotely addresses privacy issues. Other resource materials were limitedly obtained from the Library of the High Court of Tanzania, Commercial Division. The researcher also accessed a report for conciliation cases (1997-2007) from the Media Council of Tanzania. Some of these cases are relevant to privacy issues.

Search engines were also instrumental to the data collection in the nature of documents. The most common tools for search of resources were the Google (http://www.google.com/) and Yahoo (http://www.yahoo.com/). Similarly, the researcher made significant use of Lexadin World Law Guide database to look for data privacy legislation and other laws regulating privacy across Africa. Europa databases[238] played a useful role in obtaining official documents, legislation and treaties, ECJ decisions, policy papers, working papers, communications, etc for European Union (EU) institutions. Equally important were the Asia Pacific Economic-Cooperation (APEC) databases (http://www.apeccp.org.tw/) which provided access to similar documents as Europa databases. The researcher put much interest on the APEC Privacy Framework. It is important to note that the list of sources of documents provided here (accessed electronically or in print) is not comprehensive. It only serves as the main sources.

The electronic sources of documents relied in this study have limitations. The first limitation is the determination of authority and authorship. With exception of official websites, materials accessed from either personal sites or blogs presented a great deal of difficulties in identifying the authority as well as authorship. In order to deal with such problems, the researcher scrutinised the sites as well as the materials using criteria set out in figure 1 of this thesis. In event the site or materials accessed from there failed to pass such criteria they were either discarded or read for

[238] See the link at http://europa.eu/documentation/order-publications/databases-alphabetical/index_en.htm.

information only. However such materials could not be relied as authoritative sources worth of being cited in the study.

The second limitation relates to the currency of information. It is important to note that not all old information is bad. Sometimes we need old information in order to trace the development of law or a particular phenomenon. Despite that, it is difficult sometimes to find the date of publication of information on materials posted on the Internet. This makes it even harder to tell the oldness or newness of the information. To deal with this problem, efforts were made to look for the date of publication of information and when that was last revised. When this was lacking, then a comparison of the source with other information already at hand was made to determine the currency of the information.[239] Commentators suggest that in order to deal with the problem of currency, the date when the website carrying the information was last revised should be looked at.[240] It is arguable that sometimes the date of the last revision of the website does not correspond with the information it contains. For example, although the Lexadin World Law Guide bears the 1 January 2011 as the last update for legislation in Seychelles, the website does not list Data Protection Act 2003[241] [242] as one of the country's legislation. Faced with a situation like this, the researcher made alternative use of search engines especially Google.com to get some clues about the information searched. Again, in order to indicate the limitation of information the researcher always recorded the date on which he reviewed information from an Internet source.[243] This was important to include when citing to the Internet resources because of their transitory nature.[244]

There is also the problem of objectivity of the sources. This, of course, depends on the nature of topics and the main agenda of the sponsors of websites. For example, issues of politics, culture or religion attract a lot of biasness because of diversities of ideas, opinion, etc. Sometimes it may only be the sponsor of a website's goals to perpetuate his or her agendas. With this in mind, and especially privacy issues concern as well people's cultures, materials accessed were objectively evaluated using criteria set in figure 1.

---

[239] Karanja, S.K., 'Schengen Information System and Border Control Co-Operation: A Transparency and Proportionality Evaluation', PhD Thesis, Faculty of Law, University of Oslo, 2006, p.18.
[240] Ibid.
[241] Act No. 9 of 2003, the Seychelles comprehensive legislation regulating use of automatically processed information relating to individuals and provision of services in respect of such information.
[242]See, http://www.ilo.org/dyn/natlex/country_profiles.nationalLaw?p_lang=en&p_country=SYC, last visited 27/09/2011.
[243] Watson, C. A., 'Internet Research Methodology', 2004 Presentations, Paper 8, p.7, http://digitalcommons.law.uga.edu/speeches/8; See also http://works.bepress.com/carol_watson/4, last visited 26/09/2011.
[244] Ibid.

Apart from the above limitations, it is also important to note that some electronic materials are copyrighted and require a subscription. The subscription usually requires one to pay for user licence or subscribe in a manner that requires payment of licensing fee. Faced with this situation, the researcher had first to consider the relevancy of the material to his study. This was done through reading the abstracts, preface of the materials or summary part of the source. Second, the material was checked from all the libraries and electronic sources the researcher had access to. If this was not found, then the researcher borrowed the materials through interchange library arrangements of those libraries he had membership. In extreme cases, the researcher had either to buy the material from bookstores or purchase the user licence to access the material online.

However, despite its limitations, the Internet provided an important source of the materials used in this thesis. To ensure that such information was accurate, authentic, authoritative, objective, relevant and current, criteria set out in figure 1 were used to evaluate such information. Nonetheless, materials in print format accessed offline (non-electronic libraries and bookstores) were equally important in providing useful information required in the analyses of this study.

Figure 1: Assessment Criteria for the Quality of Internet Sources

Criteria	Description
Authority	o Credentials of the author or website o Author's educational background o Past writing and experience in the field o Author's institutional affiliation o Author's contacts o Author's signature on the work
Authenticity	o Look under links with titles like "More about us", or "About this site. o Go to the home page of the site sponsor if the documentation is not evident on the page you enter the site. o If you cannot determine the author or publisher of a site, examine the structure of the web address. Many web addresses are readily identifiable by their extensions. For example: gov = government, edu = educational institution, org = nonprofit organization, com = commercial organization. Similarly a web address with a tilde (~) is primary evidence that the web page is an unofficial, unauthorized or personal page.
Accuracy	o Do you recognize the name of the publisher or author? If not, does the publisher provide verifiable evidence of its competency? o Are there citations to other published works, a corporate profile, and information about editorial standards? o If you have never heard of the author, does she supply an autobiography or curriculum vita containing verifiable evidence of her authority on the subject? o Examine the names of individuals or groups responsible for information supplied by the site. A credits and conditions statement might offer this information.
Currency	o Date of publication o Date of revision o What has been revised?
Relevancy	o Is there a bibliography? o Does it provide new/add to/substantiate information at hand? o Is the material primary or secondary? o Audience o Is the work reviewed or referred? o Able to verify through traditional edited print or electronic source? o Are there errors which may affect accuracy or information?

Source: adopted partly from Karanja[245] and Watson.[246]

[245] Karanja, p.17, note 239, supra.
[246] Watson, note 243, supra.

Interviews for this research were carried out in Mauritius, South Africa and Tanzania between 28 June and 16 September, 2011. These interviews were unrepresentative and non-random. Three categories of interviewees were involved: key informants (usually academics, researchers, national officials responsible for the law reform commissions, data privacy offices, commissions for human rights, attorney general's offices, judiciary and legislators), data controllers(public and private organisations as well as individuals), and data subjects. Initially a total number of 15 respondents in each country case study reflecting the above categories were planned. However, in the course of field research and especially after interviewing key informants, adjustments were made to the plan.

In South Africa, key informants interviewed were Professor Anneliese Roos at UNISA and Professor Iain Currie at WITS. The researcher has been in contact with Roos since September 2008 by email communications. This was the time he was developing literature review of a project proposal of this thesis. So far the researcher is aware that Roos is the first to carry out scientific research on data privacy protection in Africa. Although her thesis is purely theoretical, 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study',[247] making comparison of South Africa's legal system with regard to protection of personal data with three jurisdictions: United States of America, United Kingdom and Netherlands, it provides an in-depth analysis of the South African system of data privacy protection. Interview with Roos provided abundant information for this thesis. As pointed out, Roos made also available to the researcher some of her published articles that were relevant to the present thesis. Equally important information was obtained through interview with Currie. The researcher came to know and contact Currie much earlier in September 2006. The researcher's contact with Currie was facilitated by Professor Lee Bygrave. Since 2006, the researcher made follow up to the South African discussions about the development of the data privacy law. Apart from being academician at WITS, Currie was also a member of the South African Law Reform Commission's project committee on privacy and data protection from 2001 to 2009.[248] It was this committee which was responsible for all preparatory works which culminated to the Protection of Personal Information Bill (B9-2009), which is yet under consideration by the South

[247] Roos, note 2, supra.
[248] South African Law Reform Commission, Privacy and Data Protection (Project 124), see also Currie, I., 'The Protection of Personal Information Act and its Impact on Freedom of Information', University of the Witwatersrand, Johannesburg, http://www.opendemocracy.org.za/wp-content/uploads/2010/10/The-Protection-of-Personal-Information-Act-and-its-Impact-on-Freedom-of-Information-by-Iain-Currie.pdf,
last visited 27/09/2011, footnote *.

African Parliamentary Portfolio Committee on Justice and Constitutional Development. Similarly, Professor Currie made available to the researcher his publications on privacy.

It imperative to note from the Discussion Paper[249] of the Privacy and Data Protection Project 124, that the South African Law Reform Commission made extensive efforts to publicise the Issue Paper[250] and to solicit response from interested persons and organisations as well as from members of the public, as to their views and opinion over regulation of individual's privacy. Written comments were received by the Commission from 34 persons and institutions.[251] The researcher obtained access to all these written comments. It is worth noting that after receiving these written comments, the South African Law Reform Commission made numerous follow-up discussions, meetings and presentations all of them resulted into publication of the Discussion Paper. The Discussion Paper was also available to the researcher. As was the case with the Issue Paper, the Discussion Paper, with proposed draft privacy legislation, was published for general information and comments.[252] During March and April 2006 the Commission held regional workshops countrywide where members of the Project Committee were present to explain and discuss the proposed options for the law reform and to note comments.[253] The initial closing date for comments to the Discussion Paper was extended (on public request) from 28 February 2006 to 30 September 2006.[254] A total of 63 written comments were received by the Commission.[255] The researcher got access to these written comments as well as the entire Commission's report on Project 124. Apart from these documents, and as pointed out, the researcher obtained access to the written proceedings and deliberations of the South African Parliamentary Portfolio Committee on Justice and Constitutional Development on the South African data privacy Bill. This access was through free subscription to the South African Parliamentary Monitoring Group.[256] With this information at the disposal of the researcher, it was considered less fruitful to conduct extensive interviews as planned.

---

[249] South African Law Reform Commission, Privacy and Data Protection, Project 124, Discussion Paper 109, October 2005, paragraph 1.4.1, http://salawreform.justice.gov.za/dpapers/dp109.pdf last visited 27/09/2011.
[250] South African Law Reform Commission, Privacy and Data Protection, Project 124, Issue Paper 24, September 2003, http://salawreform.justice.gov.za/ipapers/ip24_prj124_2003.pdf last visited 27/09/2011.
[251] South African Law Reform Commission, Discussion Paper 109, paragraph 1.4.3.
[252] South African Law Reform Commission, Privacy and Data Protection, Project 124, Report, August 2009, paragraph 1.4.4,
http://salawreform.justice.gov.za/reports/r_prj124_privacy%20and%20data%20protection2009.pdf,
last visited 27/09/2011.
[253] Ibid, paragraph 1.4.5.
[254] Ibid.
[255] Ibid.
[256] Note that the researcher has continued to have this access to date. Because of this, he has been able to follow future proceedings and deliberations of the Portfolio Committee even after the field research period was over.

In Mauritius, the researcher's key informant was the Data Protection Commissioner (Mrs. Drudeisha Madhub).[257] She is the first Mauritian Data Protection Commissioner to be appointed to head the Data Protection Office.[258] The researcher established contacts with Mrs. Madhub on 26 January 2011. Interview with Mrs. Madhub was conducted on 4 July 2011 in her office in Port Lois. Most of her responses transcended the questions reserved for data controllers and subjects. Again, privacy complaints lodged with the Data Protection Commissioner by data subjects as well as decisions already passed by the Commissioner were sufficient to provide a broad light as to data subjects' attitudes towards their privacy. The researcher was availed with all the decisions by the Commissioner. Since these decisions are also freely accessible online, the researcher has been able to access new decisions that were decided after the field research period was over. Moreover, the Commissioner availed the researcher all her written presentations made to public and private organisations as well as general public about the data protection Act. They were about twenty two presentations. Based on these resources, the researcher conducted few interviews with individuals in public places.

In Tanzania, interviews were held with the following institutions: the Tanzania Communications Regulatory Authority (TCRA), Law Reform Commission (LRC), Commission for Human Rights and Good Governance (CHRAGG), Zantel (a mobile communication company) and individuals. At TCRA, the researcher interviewed the Deputy Director (Consumer Affairs), Mr. Richard Kayombo. Since TCRA is the communication regulator, most information gathered from this interview concerned consumer privacy right in the communication sector. The researcher was also availed information about privacy complaints lodged with the authority. He also accessed various documents on consumer rights generally and on privacy in particular from the authority's website. At LRC, the researcher interviewed the Deputy Executive Secretary of the Commission, Mr. Adam J. Mambi. Apart from being LRC's Deputy Executive Secretary, Mr. Mambi served as a member of the Task Force that dealt with development of cyberlaws (including data privacy laws) in the East African Community. At CHRAGG, the Principal Computer System Analyst, Mr. Wilfred Warioba, was interviewed. At Zantel, the researcher interviewed the Company's Data Manager, Mr. Abdillah Kiiza Abdillah. The information collected from these sources left the researcher with a little task of interviewing individuals.

[257] Mrs. Madhub formerly worked with the Mauritian Attorney-General's Office as a Senior State Counsel.
[258] One of the principal functions of the Commissioner is to enforce the Mauritian Data Protection Act 2004, see S. 5.

As a whole, interviews with respondents were informal and semi-structured. Three set of pre-designed questions for key informants, data controllers and data subjects were used as guides. Upon request, some interviewees were sent list of questions in advance for making thorough preparation. However during interview, supplementary questions were asked by the researcher. Such questions mostly emerged from the interviewees' responses. Sometimes the researcher reserved sensitive questions for the actual interview session. It is worth noting that some interviewees preferred to fill pre-designed questions. Nevertheless, such interviewees were still willing to accommodate researcher's new and supplementary questions. Finally, the interviewees were friendly and cooperative to the researcher.

1.2.4.3 Comparative Legal Research

Since its inception in the 20th Century, comparative law has played significant role in the science of legal interpretation in national courts, legal reforms as well as unification and harmonisation of laws.[259] Summarising the role of comparative legal analysis Wilson posits, 'by looking overseas, by looking at other legal systems, it has been hoped to benefit the national legal system of the observer, offering suggestions for future developments, providing warnings of possible difficulties, giving an opportunity to stand back from one's own national system and look at it more critically, but not to remove it from first place on the agenda.'[260] [261] It is widely acknowledged that, data privacy issues are becoming more and more international. Article 25 of the EU Data Privacy Directive has to the greatest extent influenced the international character of data privacy law. It has imposed a condition for non-EU countries to implement mechanisms for protection of privacy that would be considered "adequate" by the EU if such countries were to continue to receive personal data from EU. This made it imperative to engage comparative legal analysis in order:-

[259] For detailed discussion about the role and function of comparative law see, Hey, E. and Mak, E., 'Introduction: The Possibilities of Comparative Law Methods for Research on the Rule of Law in a Global Context', Erasmus Law Review, 2009, Vol. 2, No. 3, pp.1-3; Dann, P., 'Thoughts on a Methodology of European Constitutional Law', German Law Journal, 2005, Vol. 6, No. 11, pp.1461-1467; Church, J. *et al.*, Human Rights from a Comparative and International Law Perspective, UNISA Press, Pretoria, 2007; Wilson, G., 'Comparative Legal Scholarship' in W.H Chui, and M. McConville, (eds), Research Methods for Law, Edinburgh University Press, 2010, pp. 87-103; Roos, pp.20-22, note 2, supra.

[260] Wilson, p.87, note 259, supra.

[261] For critical works on comparative legal research, see for example, Kiekbaev, D.I., 'Comparative Law: Method, Science or Educational Discipline?', Electronic Journal of Comparative Law, 2003, Vol. 7.3, <http://www.ejcl.org/73/art73-2.html>, last visited 27/09/2011.

- To compare the regimes of data privacy at the international and regional level outside Africa. Such comparison was necessary to understand the legal principles incorporated in the international and regional data privacy instruments.

- To compare the national systems of data privacy protection and practices in the three country case studies in sub-Saharan Africa.

To achieve the above goals, the following instruments were reviewed: treaties, conventions, guidelines, directives, frameworks and agreements laying down the data protection and privacy principles at regional and international level. At national level comparison was made especially on constitutions, legislation, regulations, case law, Bills, and institutions of enforcement of privacy.

1.2.5 Chapter Overview

This thesis is divided into eight chapters. Chapter 1 comprises the *Introduction*. It generally sets out the research agenda of the present study. Specific issues covered in this chapter include the research problem. This chapter also covers the research questions guiding this study as well as the methodology of research. Apart from that, it deals with literature survey relevant to the research problem. Chapter 2 is headed *Concepts and Theories of Privacy*. It revisits various concepts and theories underpinning privacy and data protection generally. Since there are myriad concepts and theories, chapter 2 delimits and rationalises the use of various concepts and theories in the context of this thesis. Chapter 3, *Privacy and Data Protection in International Law*, sketches the systems of privacy and data protection as provided for in the international and regional instruments. The rationale behind the inclusion of this chapter is that most national privacy and data protection legislation across the world owe their origins from the international and regional instruments. Because of this, the frameworks of these instruments are important as they lay down the foundation for discussion in subsequent parts of this thesis. Chapter 4, *Privacy and Data Protection in Africa*, addresses generally the origins and state of the right of privacy in Africa, the general social attitude of Africans towards privacy as well as factors affecting such attitudes, existing legislative protection and their limitations, sub-regional as well as national efforts towards adoption of data privacy legislation. Chapter 5 covers *Data Protection in Mauritius*. It focuses on Mauritian data privacy legislation. Moreover, chapter 5 briefly covers other legislative and non-legislative instruments regulating protection of privacy. The enforcement of the data

privacy legislation by the Data Protection Commission is discussed in detail to understand the data protection practice in the country. Chapter 6, *Data Protection in South Africa*, focuses on the South African Bill on protection of privacy. The legislative process of this Bill is fully discussed. Moreover, this chapter reviews the socio-economic political context of South Africa under the *apartheid* and assesses how such context has influenced the adoption of the privacy law in the country. Other statutes addressing privacy issues as well as common law are discussed as well. Chapter 7, *Data Protection in Tanzania*, deals with privacy and data protection in a jurisdiction which has neither a data privacy law nor Bill on such legislation. *Ujamaa* ideology is assessed here in the context of concerns for privacy. The current system of privacy protection is covered as well. Chapter 8, *Comparative Conclusions*, summarises the main points covered in the previous chapters and offers the major findings of the study. It also outlines the future research agenda.

1.2.6 Conclusion

Data protection in Africa is in a nascent growth. So far only eleven countries have implemented omnibus data protection legislation from 2001 to 2012. This number is likely to increase in a near future as some African countries are in the legislative process of such laws. Scholars have advanced various explanations as to the state of privacy in Africa. Central to them is the culture of collectivism. However other explanations advanced for the state of data privacy in Africa, particularly economic outsourcing, are external to the culture of collectivism. This study ventures to merge this *lacuna* in the discourse of data privacy in Africa. The research problem, research questions and methodology have been extensively and systematically covered to reflect the scope of the study.

2. Concepts and Theories of Privacy

2.1 Introduction

This chapter examines concepts and theories of privacy. Two key concepts namely *privacy* and *data protection* as prominently manifesting in the privacy and data protection discourse are primarily the focus in section 2.2. Other concepts considered here include *data privacy*, *information privacy*, *informational autonomy*, *personal data, personal information*, *data subject*, *data controller*, *data processor* and *data processing*. Apart from that, section 2.2 addresses the problem of nomenclature. Section 2.3 sets out and discusses various theories of privacy. Although there are myriad theories on privacy, only six of them are examined since they overlap at some points. This section also canvasses the strengths and weaknesses of these theories. It is noteworthy that most of the theories covered here were postulated by Western scholars. This section leaves unexamined concepts and theories that specifically attempt to define data privacy in the African context. Discussion on the latter is purposely reserved for chapter four. Section 2.4 deals with choice of terminologies and theories as used in this thesis. Finally, section 2.5 concludes this chapter.

2.2 Concepts and the Problem of Nomenclature

Privacy and *data protection* are said to belong to the two sides of the Atlantic. While the term *privacy* is widely used in USA, Canada and Australia[262] the term *data protection* is commonly used in European jurisdictions.[263] Nevertheless, this territoriality use of the two terms is problematic for two reasons. First, it fails to tell the inherent similarities and differences between the two concepts. Second, at some point the two terms find their ways to the opposite side of the Atlantic, henceforth exist simultaneously side-by-side. With this situation, commentators strive to find clear-cut limits of these concepts without success. While some tend to view the two concepts as synonymous hence interchangeable others maintain the opposite views. Sometimes commentators end in frustration with a failure to clearly point out the differences between these concepts. For example, Kuner observes:-

> 'In European law, "privacy" includes issues relating to the protection of an individual's "personal space" that go beyond data protection, such as "private, family and home life, physical and moral integrity, honour and reputation,

[262] Note that although Australia does not belong to either side of the Atlantic in the strict sense of the term it employs the term 'privacy' largely because of the influence from the American and Canadian jurisprudence.
[263] Bygrave, p.1, note 24, supra.

> avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially. In the United States, the US Supreme Court has interpreted the Constitution to protect, under the rubric of "privacy", values that go beyond the protection of personal data, such as an individual's constitutional right to be free from unreasonable searches and seizures by the government, the right to make decisions about contraception, abortion, and other intensely personal areas such as marriage, procreation, child rearing, and education, and the right to associate free from government intrusion.'[264]

He concludes that *privacy* can be seen as a concept which is both broader than and independent from *data protection*, though there can be a significant overlap between the two.[265]

An attempt to demarcate the domains of the two concepts i.e. *privacy* and *data protection* is also undertaken by Cuijpers who raises a question, 'is the right to data protection the same as the right to privacy?'[266] In response, he subscribes his views to Peter Block that *data protection* and *privacy* are not the same. The two argue that since individual right to privacy safeguards an undisturbed private life and offers the individual control over intrusion of the private sphere, it is different from protection of the individual with regard to the processing of personal data which is not restricted to the private sphere of the individual.[267] Accordingly, they conclude that the choice to link *data protection* to the right to *privacy* is unjustly made.[268] Similarly but in somewhat confusingly manner, De Hert and Schreuders argue that although *data protection* and *privacy* share certain features and goals, and are frequently used as synonyms, they are not identical.[269] They are therefore described as being 'twins, but not identical'.[270] These scholars continue to argue that although clearly engrained in privacy protection, *data protection* does not necessarily raise *privacy*

---

[264] Kuner, C., 'An International Legal Framework for Data Protection: Issues and Prospects', Computer Law & Security Review, 2009, Vol. 25, No.4, pp.307-317, at p. 308.
[265] Ibid.
[266] Cuijpers, C., 'A Private Law Approach to Privacy: Mandatory Law Obliged?', SCRIPTed, 2007, Vol.4, No.4, pp.304-318, at p.312.
[267] Ibid.
[268] Ibid.
[269] De Hert, P and Schreuders, E., 'The Relevance of Convention 108', 33,42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19-20, November, 2001 cited in 'EU Study on the Legal Analysis of a Single Market for the Information Society', November, 2009, Chapter 4, p.4.
[270] Ibid.

issues.[271] Contrary to privacy rules, data protection rules are not prohibitive.[272] Instead, they organise and control the way personal data can only be legitimately processed if some conditions pertaining to the transparency of the processing, the participation of the data subject and the accountability of the data controller are met.[273] In the same vein De Hert and Gutwirth argue:-

> 'Data protection is a catch-all term for a series of ideas with regard to the processing of personal data. By applying these ideas, governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc. In general, data protection does not have a prohibitive nature like criminal law. Data subjects do not own data. In many cases, they cannot prevent the processing of personal data. Under the current state of affairs, data controllers (actors who process personal data) have the right to process data pertaining to others. Hence, data protection is pragmatic; it assumes that private and public actors need to be able to use personal information because this is often necessary for societal reasons. Data protection regulation does not protect us from data processing but from unlawful and/or disproportionate data processing.'[274]

In further differentianting *privacy* from *data protection*, De Hert and Gutwirth observe:-

> 'Data protection's real objective is to protect individual citizens against unjustified collection, storage, use and dissemination of their personal details. This objective seems to be indebted to the central objective of the right to privacy, to protect against unjustified interferences in personal life. Many scholars therefore hold data protection and privacy to be interchangeable.'[275]

The authors argue that equating *privacy* and *data protection* on the basis of the objectives each wants to achieve is a narrow view. To the contrary De Hert and Gutwirth hold that there are

---

[271] Ibid.
[272] Ibid.
[273] Ibid.
[274] De Hert, P and Gutwirth, S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action', in Gutwirth, S *et al* (eds)., Reinventing Data Protection?, Springer, 2009, pp.3-44 at p. 3.
[275] Ibid, p.4.

important differences between the two in terms of scope, goals and content.[276] By subscribing to Bygrave's views extracted from his article, 'The Place of Privacy in Data Protection Law',[277] De Hert and Gutwirth argue that while privacy obviously occupies a central place in data protection law, their characterisation of data protection law as solely or even essentially concerned with safeguarding privacy is misleading.[278] Data protection laws serve a multiplicity of interests, which in some cases extend well beyond traditional conceptualisations of privacy.[279]

Yet, between the two ends of the spectrum there are commentators who, in an attempt to reconcile the opposite views, have invented new concept *data privacy*.[280] Bygrave argues that in contrast to the concept *data protection* which fails to indicate the central interests served by the norms to which it is meant to apply, *data privacy* is more appropriate as it better communicates the central interest(s) at stake and provides a bridge for synthesising North America and European policy discussion.[281] While this view is meritorious, other commentators tend to use an alternative concept of *information privacy* for the above discussed sense. Karanja, for example, argues:-

> 'The concept "information privacy" is concerned with the protection of personal data. In Europe, the term "data protection" is used to refer to "information privacy". Although the two concepts, information privacy and data protection, may differ somewhat in meaning and the scope of the former being wider than the latter (sic). Both expressions are used interchangeably to refer to the same thing-protection of personal data.'[282]

In the *Death of Privacy*, Froomkin uses the concept *information privacy* as shorthand for the ability to control the acquisition or release of information about oneself.[283] As it is explained in 2.3, Froomkin's understanding of *information privacy* is a reflection of the privacy control theory. It is noteworthy that the use of *information privacy* in the context of *data protection* is an attempt to limit the broader concept of *privacy*. Such a broader concept of *privacy* is explained briefly by the

---

[276] Ibid, p.9.
[277] Bygrave, L. A, 'The Place of Privacy in Data Protection Law' University of New South Wales Law Journal, 2001, Vol. 24, No. 1, pp. 277-283, at p. 282.
[278] De Hert and Gutwirth, p.10, note 274, supra.
[279] Ibid.
[280] Schwartz, P.M and Reidenberg, J.R., Data Privacy Law: A Study of United States Data Protection, Michie Law Publishers, Charlottesville, 1996, p.5.
[281] Bygrave, pp.321-322, note 25, supra.
[282] Karanja, p.86, note 239, supra.
[283] Froomkin, note 7, supra.

Electronic Privacy Information Centre and Privacy International in their 2006 report on worldwide surveys of privacy and human rights.[284] According to this report, *privacy* is classified into four aspects. These include: first, *information privacy*, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as *data protection*; second, *bodily privacy*, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches; third, *privacy of communications*, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and forth, *territorial privacy*, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.[285] From this classification, it is the first aspect, i.e. *information privacy* which is equated to data protection. The other aspects: *bodily privacy*, *privacy of communications* and *territorial privacy* are excluded from the purview of *data protection*. However, in contrast to the above, other commentators such as Kuhlen conceive the concept of *privacy* not primarily in the sense of *data protection* or of the 'right to be let alone' but of what in Germany is called *informational autonomy* (i.e. *informationelle Selbstbestimmung*).[286] The latter is understood as the capacity to choose and use autonomously knowledge and information in an electronic environment.[287]

Attempts to demarcate the realm of *privacy* from that of *data protection* have also been made using case law of the European Commission and Court of Human Rights (ECtHR) interpreting the right to privacy enshrined in Human Rights Treaties. The latter include Arts 17 and 8 of the International Covenants on Civil and Political Rights (ICCPR) 1966 and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) 1950 respectively. Though there seems to be consensus among commentators on the limitations of the Strasburg privacy case law in spelling data protection principles, the reasoning has varied significantly. For example, in summing the limited scope of the Strasburg case law in relation to data protection, Bygrave argues:-

---

[284] Electronic Privacy Information Centre and Privacy International (PI), 'Overview of Privacy' in Privacy and Human Rights Report, 2006, https://www.privacyinternational.org/article/phr2006-overview-privacy last visited 23/10/2011.

[285] Ibid.

[286] Capurro, R., 'Privacy: An Intercultural Perspective', Ethics and Information Technology, 2005, Vol.7, No.1, pp.37-47, at p.40.

[287] Kuhlen, R., Informationsethik. Umgang mit Wissen und Information in elektonischen Räumen.UTB: Universitätsverlag Konstanz, Konstanz 2004 cited in Capurro, R., 'Privacy: An Intercultural Perspective', Ethics and Information Technology, 2005, Vol.7, No.1, pp.37-47, at p.40

> 'At present, the case law developed around the right to privacy in Art 17 of the ICCPR and Art 8 of the ECHR falls short of explicitly stipulating data protection guarantees as comprehensive as those found in instruments concerned specifically with data protection. Moreover, the case law is somewhat confusing: the principles for processing personal data which emerge from it are often sketchy and of little prescriptory value. This is so even with the relatively extensive body of case law developed around Art 8 of the ECHR. Too often there has been failure by the Commission and/or Court to make clear exactly which elements of the contested data-processing practice has interfered with the right under Art 8(1); too often has there been a concomitant failure to describe the threatened interest.'[288]

However, Bygrave notes that the omitted prescriptory value of Art 8 case law in the field of data protection is not simply due to the Commission and Court.[289] It is also due to the fact that a large proportion of the case law concerns data processing in a rather special context (i.e., secret surveillance activities by police or intelligence agencies), while almost none of it deals with private entities' data-processing practices.[290] Despite these limitations, Bygrave is optimistic that the willingness of the Strasburg organs to adopt data protection provisions which grow nationally and internationally, these organs will increasingly expand the right to privacy in the light of these laws.[291] Bygrave's optimisms became a reality seven years later. In his analyses of the case law of the ECtHR, Karanja summarises the value of this case law in relation to data processing practices as follows:-

> 'Going by the recent case decisions of the ECtHR, it is no longer doubtful that data protection is a human right although the Convention does not state this. As indicated above, the Court has boldly manifested data protection principles in its decisions by adopting the language of data protection law. But what still lacks in the Council of Europe human rights framework is a positive statement in the general human rights legislation that human rights protects

[288] Bygrave, L.A., 'Data Protection Pursuant to the Right in Human Rights Treaties', International Journal of Law and Information Technology, 1998, Vol.6, No.3, pp.247-284, at pp.283-284; see also, Ulyashyna, L., 'Does case law developed by the European Court of human Rights pursuant to ECHR Article 8 add anything substantial to the rules and principles found in ordinary data protection principle?', A Tutorial Paper presented at the Norwegian Centre for Computers and Law(NRCCL), Spring, 2006.
[289] Bygrave, note 288, supra.
[290] Ibid, p.284.
[291] Ibid.

> personal data. Such statement would give data protection the universal status enjoyed by human rights principles. The EU has cured the anomaly by enacting a data protection provision in its Charter of fundamental rights and the EU Constitution."[292]

It is noteworthy that the above views by Karanja are in sharp contrast to the observation of the European Court of First Instance in *Bavarian Lager Co. Ltd v Commission.*[293] In this case the Court observed, 'it should also be emphasized that the fact that the concept of "private life" is a broad one, in accordance with the case-law of the European Court of Human Rights, and that the right to the protection of personal data may constitute one of the aspects of the right to respect of private life...does not mean that all personal data necessarily fall within the concept of "private life".'[294] Moreover, recently De Hert and Gutwirth have critically evaluated the case law of Strasburg only to find that such case law not only fails but also lacks any potential of embracing data protection principles. These scholars have advanced three reasons to support their claims. First, there are comparatively few Strasburg's judgments that offer criteria for excessive, unnecessary and/or unjustified collection of personal data.[295] According to them, this is owing to the fact that the Court makes overstretched focus on the legality requirement.[296] Second, based on the scholars' experience of this case law, they believe that many Court judgments allow processing authorities too much leeway.[297] Only flagrant abuse or risky use of data which is easily used in a discriminatory way is very closely scrutinised, whereas other kinds of processing of data are left untouched 'as long that there is no blood'.[298] Third, the very basis of data protection recognition in Strasburg is not as solid as it looks.[299] For example, the ECtHR has once stipulated that Art 8 of ECHR does not give a general right to access personal data contrary to the data protection instruments.[300] Also, the Court has made a distinction between personal data that fall within the scope of Art 8 of the ECHR and personal data that do not.[301] De Hert and Gutwirth thus observe that in the eyes of the Court there is processing of personal data that affects private

---

[292] Karanja, p.123, note 239, supra.
[293] Case T-194/04, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004A0194:EN:HTML last visited 23/10/2011. Judgment was delivered at Luxembourg on 8 November 2007.
[294] Ibid, paragraph 118 of the Judgment.
[295] De Hert and Gutwirth, p.23, note 274, supra.
[296] Ibid.
[297] Ibid.
[298] Ibid.
[299] Ibid, p.24.
[300] Ibid; see also Gaskin v. United Kingdom, ECtHR, Strasburg, Application No. 10454/83[1989], paragraph 37 of the judgment.
[301] Ibid, pp.24-25.

life and processing of personal data that does not affect the private life of individuals contrary to the general protection of all personal data offered by data protection regulations.[302]

An overview of the understandings attempting to distinguish *privacy* from *data protection* reveals three important conclusions. First, in strict sense *privacy* and *data protection* are two distinct and separate concepts though they have overlapping objectives. The differences between the two concepts reside in their scope, goals and content. However, it is important at this juncture to argue that those attempts which differentiate *privacy* from *data protection* pointing out that the former is prohibitive while the latter is not, are illusive. For example, one of the mandatory legal preconditions for processing personal data in the Directive 95/46/EC is consent.[303] The notion of consent is traditionally linked to the idea that the data subject should be in control of the use that is being made on his data.[304] In turn, the notion of control is linked to the fact that the data subject should be able to withdraw his consent consequently preventing any further processing of the individual's personal data by the data controller.[305] Also, consent is related to the concept of informational self-determination making the autonomy of the data subject both a pre-condition and a consequence of consent.[306] In essence, consent gives the data subject influence over the processing of data.[307] However, although consent is one of the legal preconditions for processing personal data, it is not absolute. Sometimes the data subject's consent is difficult to attain in real life[308] or it is subject to exemptions for purposes of public interests such as defence and national security. Notwithstanding, it is arguable that consent is prohibitive to data processing activities equating *data protection* to *privacy* to that extent. A slight but similar view is maintained by De Hert and Gutwirth though they generally view *privacy* as prohibitive as opposed to *data protection*. These scholars argue that data protection also prohibits certain processing of personal data, for instance 'sensitive data'.[309] The second conclusion drawn from the above discussion about *privacy* from *data protection* is that, the two concepts are increasingly

---

[302] Ibid; see also Pierre Herbecq and the Association Ligue des droits de l 'homme v Belgium. Cf. ECommHR, Pierre Herbecq and the Association Ligue des droits de l 'homme v Belgium, Decision of 14 January 1998 on the applicability of the applications No. 32200/96 and 32201/96(joined), Decisions and Reports, 1999, paragraphs 92-98.

[303] See for example, Art 7(a) & 8(2), (a) of the Directive 95/46/EC.

[304] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent', 01197/11/EN, WP187, p.8, (adopted 13th July 2011).

[305] Ibid, p.9.

[306] Ibid.

[307] Ibid.

[308] See e.g Elahi, S., 'Privacy and Consent in the Digital Era', Information Security Technical Report, 2009, Vol.14, No.3, pp.113-118, at p.115; see also, Whitley, E.A., 'Informational Privacy, Consent and the "Control" of Personal Data', Information Security Technical Report, 2009, Vol.14, No.3, pp.154-159, at pp. 155-156.

[309] De Hert and Gutwirth, p. 4, note 274, supra.

becoming synonymous and hence interchangeable in their daily uses. As rightly observed by Kuner:-

> 'Calls for an international framework have tended to mix the terms "data protection" and "privacy". For example, the resolution approved at the 30th International Conference in Strasburg quoted above refers to "the rights to data protection and privacy", while the principles adopted by the "Global Network Initiative", a group formed by a number of companies, non-governmental organizations, and academics, deal with "the internationally recognized human rights of freedom of expression and privacy", thus focusing more on privacy than on data protection. The "Global Privacy Standard", published in November 2006 by a working group led by Ontario Information and Privacy Commissioner, refers many times to "privacy", but the principles themselves deal with topics such as consent, purpose limitation, and access rights, that have traditionally been thought to be key concepts of data protection law.'[310]

The New Zealand Privacy Act 1993 is also instructive to illustrate the mixed use of the concepts *privacy* and *data protection*. Despite its reference to privacy in its short title, the Article 29 Working Party made key findings in its one of the most recent opinion on 'adequacy'.[311] First, the Privacy Act is the main New Zealand data protection legislation. The latter has been heavily influenced by the 1980 *OECD Guidelines*. Though the Privacy Act predates the Directive 95/46/EC, still the Working Party considered New Zealand to meet the 'adequacy' standard set to evaluate non-EU member states with regard to their data protection laws and practices. This means that the New Zealand Privacy Act contains data protection principles notwithstanding its privacy name. The third conclusion is that when the context in which the concepts *privacy* and *data protection* are used is not provided, one has to carefully scrutinise the contents of the principles covered, their scope and application. This is important because sometimes the true context in which these concepts are used need to be identified in order to ascertain consequential implications from their application.

---

[310] Kuner, note 264, supra.

[311] Article 29 Data Protection Working Party, 'Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand', 00665/11/EN, WP182, pp.2&15, (adopted on 4th April 2011).

Not all concepts in the privacy and data protection discourse present difficulties to define. The more obvious of them include *data subject*. It refers to an individual whose personal information is subject to data processing activities.[312] In some jurisdictions the term *data subject* applies to firms and legal entities which in law enjoy legal personality.[313] *Data controller* may be a natural person or legal entity which controls and determines the purpose and means of processing personal data belonging to *data subjects*.[314] In practice a *data controller* engages other persons to carry out processing on his or her behalf. Such persons or legal entities processing personal data on behalf of a *data controller* are called *data processors*.[315] However it must be pointed out that in 2010, the Article 29 Working Party issued opinion trying to clarify the meaning of *data controller* and *data processor*. This opinion was triggered by organisational differentiation in the public and private sector, development of ICT as well as the globalisation of data processing, increased complexity in the way personal data are processed and call for clarifications of these concepts, in order to ensure effective application in practice.[316] According to the Article 29 Working Party, the term *data controller* is autonomous, in the sense that it should be interpreted mainly according to Community data protection law, and functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on factual rather than a formal analysis.[317] As to *data processor*, the Article 29 Working Party notes that the same way of analyzing the *data controller* should be used.[318] However, the existence of a *data processor* depends on a decision taken by the *data controller*, who can decide either to process data within his organization

[312] See e.g. Directive 95/46/EC, Art 2(a).

[313] See e.g. South African Protection of Personal Information Bill (B9-2009), s.6; see also Bygrave, L.A., 'A Right to Privacy for Corporations? *Lenah* in International Context', Privacy Law & Policy Reporter, 2001, Vol.8, pp.130-134; Bygrave, L.A., 'Data Protection Reforms in Scandinavia', Privacy Law & Policy Reporter, 1998, Vol.5, pp.9-12, at p.11 where Bygrave summarises the position of the law in Scandinavian countries with regard to the protection of data privacy of legal/juristic persons as follows, 'under Norway's current data protection legislation, data on private corporations and other legal/juristic persons are expressly protected to much the same extent as data on individual natural/physical persons(hereinafter termed simply "individuals"). Data on legal persons are also expressly protected under Denmark's *Private Registers Act* but not its *Public Authorities' Registers Act*; that is, the processing of legal person data by government agencies falls outside the scope of the Danish data protection regime. Even in relation to private sector data-processing practices, legal persons(as data subjects) are not provided with exactly the same rights as an individual: they do not enjoy a *general* right of access to information that other organisations keep on them; access rights are granted only with respect to information kept by credit reporting agencies. As for the situation in Sweden, the Data Act does not expressly protect data on legal persons though the latter are provided with limited data protection rights pursuant to two pieces of sectoral legislation: the *Credit Reporting Act* of 1973(*Kredituppplysningslag*,1973:1173) and *Debt Recovery Act* of 1974(*Inkassolag*, 1974:182).' Other countries outside Scandinavian region with data privacy legislation extending regulation to legal entities include Austria, Italy and Luxembourg.

[314] Directive 95/46/EC, Art 2 (d).

[315] Ibid, Art 2 (e).

[316] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts "Controller" and "Processor"', 00264/10/EN, WP164, p.1, (adopted on 16th February 2010).

[317] Ibid, p.32.

[318] Ibid, p.33.

or to delegate all or part of the processing activities to an external organization.[319] Thus, the two basic conditions for qualifying as *data processor* are on the one hand being a separate legal entity with respect to the *data controller* and on the other hand processing personal data on his behalf.[320] Other criteria advanced by the Article 29 Working Party to assist determine the different roles of parties in the data processing activities include the level of prior instruction given by the *data controller*, the monitoring by the *data controller* of the level of service, the visibility towards *data subjects*, the expertise of the parties, the autonomous decision-making power left to the various parties.[321] The ranges of operations and/or activities that are carried upon personal data are collectively known as *data processing.*[322] The latter includes collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure, erasure, destruction, blocking, dissemination, etc. It is important to note that sometimes there are variations from one jurisdiction to another regarding these terminologies. Nonetheless, the roles and positions such terminologies occupy in data protection law are materially the same in most such cases. In that connection, for example, *data medium*[323] or *responsible party*[324] or *data user*[325] has been used interchangeably with *data controller*. As to *data processor* the term *computer bureau* has been used instead in some jurisdictions.[326]

Notwithstanding the seemingly relative ease with which concepts have been defined in the preceding paragraph, the associated concept of *personal data* or sometimes referred to as *personal information* has presented most difficulties to define. So far there is no settled legal position as to the precise scope and limit of what constitutes *personal data*. For example, Wacks argues that *personal information/data* is integral to the regulation of privacy and any definition of personal information must incorporate two key elements: the quality of the information and the reasonable expectations of the individual using it.[327] He contends that personal information therefore must have both a normative and descriptive function because the notion of what is personal relates to a desired social norm (e.g. the ability to withdraw certain information about

---

[319] Ibid.
[320] Ibid.
[321] Ibid.
[322] See, e.g. Directive 95/46/EC, Art 2 (b).
[323] Neethling, J *et al*., Persoonlikheidsreg, p. 321 cited in Roos (LL.D Thesis) p. 19, note 2, supra.
[324] See, e.g. South African Protection of Personal Information Bill (B9-2009), s.1.
[325] See, e.g. Seychellois Data Protection Act, 2003, s.2 (10).; see also, the United Kingdom (UK) Data Protection Act, 1984(now repealed and replaced by UK Data Protection Act, 1998), s.1 (5).
[326] See e.g. Seychellois Data Protection Act, 2003, s.2 (11).; see also, the United Kingdom (UK) Data Protection Act, 1984(now repealed and replaced by UK Data Protection Act, 1998), s.1 (6).
[327] Wacks, R., Personal Information: Privacy and the Law, Oxford: Clarendon Press, 1993, p.24 cited in Burdon, M and Telford, P., 'The Conceptual Basis of Personal Information in Australian Privacy Law, eLaw Journal: Murdoch University Electronic Journal of Law, 2010, Vol.17, No.1, p.6; see also Wacks, R., ''Private Facts'': Is Naomi Campbell a Good Model?', SCRIPTed, 2004, Vol.1, No.3,pp.420-433, at p.431.

oneself) and to describe something as personal accords the conditions of the desired social norm (e.g. information as personal information means an individual is granted control over it).[328]

Whilst Wacks examines the normative elements of personal information, Bygrave identifies common conditions that make up personal information.[329] Bygrave notes that generally, definitions of *personal data* found in international and regional instruments as well as domestic data protection legislation are broad.[330] He argues that one can read into these definitions two cumulative conditions for data or information to be 'personal': first, the data must relate to or concern a person; secondly, the data must facilitate the identification of such a person.[331] Regarding the first condition, however, there is usually no requirement that the data relate to a particular (e.g., private, intimate) sphere of a person's activity.[332] Because of this, in most cases, it may not be appropriate to talk of two separate(though cumulative) conditions for making data 'personal'; the first condition can be embraced by the second in the sense that information will normally relate to, or concern, a person if it facilitates that person's identification.[333] In other words, Bygrave is saying, the basic criteria appearing in these definitions is that of identifiability; i.e., the potential of information to enable identification of a person.[334] In determining whether information is 'personal' i.e. if it is capable of identifying an individual, Bygrave developed six criteria in interrogative form, though he admits that such criteria are inter-related hence the answer to one partly determines the others. The six criteria are: 1) what exactly is meant by the concept(s) of identification/identifiability?, 2) how easily or practicably must a person be identified from information in order for the latter to be regarded as 'personal'?, 3) who is the legally relevant agent of identification (i.e., the person who is to carry out identification)?, 4) to what extent must the link between a set of data and a person be objectively valid?, 5) to what extent is the use of auxiliary information permitted in the identification process? Is information 'personal' if it allows a person to be identified only in combination with other (auxiliary) information? and 6) to what extent must data be linkable to just one person in order to be 'personal'?[335] He concludes as follows:-

---

[328] Ibid, (Wacks p.20/Burdon and Telford).
[329] Burdon, M and Telford, P., 'The Conceptual Basis of Personal Information in Australian Privacy Law, eLaw Journal: Murdoch University Electronic Journal of Law, 2010, Vol.17, No.1, p.6.
[330] Bygrave, p.42, note 24, supra.
[331] Ibid.
[332] Ibid.
[333] Ibid.
[334] Ibid.
[335] Ibid.

> '...it is clear that many of the definitions of personal data are capable in theory of embracing a great deal of data, including geographical and environmental data, which *prima facie* have little direct relationship to a particular person. At the same time as this capability has obvious benefits from a data protection perspective, it threatens the semantic viability of the notion of "personal data/information" and incurs a practical-regulatory risk that data protection laws will overreach themselves. Thus, in some jurisdictions, attempts have been made to limit this capability.'[336]

From the above conclusion, there is no doubt that Bygrave advocates for a limited interpretation of the concept of personal data though of course that does not necessarily mean restrictively narrowing such interpretation. This view is also correctly echoed by Burdon and Telford who seem to observe: 'He (Bygrave) argues that limitations are required to ensure the 'semantic viability' of the concept and the effective functioning of regulatory capacities required by information privacy laws'.[337]

The difficulty in defining *personal data* has been further complicated by the decision of the English Court of Appeal in *Michael John Durant v Financial Service Authority*[338] commonly referred to as the *Durant* case. This case was decided after Wacks and Bygrave's postulations of *personal data*. One of the issues dealt by the Court of Appeal and which features prominently in the Court's judgment was whether the information held by the Financial Service Authority(FSA) relating to the investigation of *Durant's* complaint constituted *personal data* under the UK Data Protection Act 1998.[339] In answering this question, the Court applied two tests cumulatively. [340] First, is whether the information alleged to relate to a particular individual in a breach of privacy complaint is biographical in a significant sense. The latter means if such information is going beyond recording of such individual's involvement in a matter or an event which has no personal connotations. Second, is the 'focus' test. This simply means that the information about a particular individual must be the 'focus' or rather central of processing and not otherwise. To put it differently, the 'focus' test requires that the individual complaining about breach of privacy must be adversely affected by the processing activities. After consideration of the parties' arguments and application of the two tests, the Court held that information about which *Durant*

[336] Ibid, p.48.
[337] Burdon and Telford, p. 6, note 329, supra.
[338] [2003] EWCA (Civ) 1746.
[339] Ibid, para 20(1) & 21.
[340] Ibid, para 28.

relied for his claim did not constitute *personal data* in the first place. This was despite the fact that the FSA investigation (from which *Durant* sought access) was triggered by the complaint lodged by *Durant* himself and also such information was retrievable by reference to his name.[341]

Commentators across Europe and USA have continuously criticised the *Durant* case for narrowing the scope of *personal data* intended to be interpreted broadly by the drafters of the Directive 95/46/EC. Room argues that the *Durant* case has effectively introduced a 'privacy filter' into the interpretation of the Data Protection Act 1998 narrowing the scope of the meaning of *personal data* to such information that only affects that individual's privacy.[342]As to why the Court preferred a narrow approach to the broad, he attributes that to the conservative attitude of the English judiciary which for quite some time has rejected the standalone notion of tort of privacy in the United Kingdom.[343] Citing *Wainwright v Home Office,*[344] Room subscribes to the line of argument taken by Helen Fenwick, in which case the author notes that the English conservative judicial attitude towards privacy has continued to prevail even after UK had adopted the Human Rights Act 1998 and the Data Protection Act 1998 which embrace privacy as a central value to be protected.[345] While Room's rationale for the *Durant's* narrow approach to the interpretation of the term *personal data* is not repeated by other authorities, generally, criticisms for the Court of Appeal's understanding of what is *personal data* has been raised from several fronts, though without further rationalisation in some cases. Yet, before *Durant* was decided, the UK Information Commissioner had already commissioned a research study to investigate into the meaning, scope and limit of the term *personal data.*[346] Unfortunately, before this study was completed the English Court of Appeal delivered its judgement in *Durant*. Perhaps if this were not the case, the Commissioner's research study into the meaning of *personal data* would have been free from the *Durant*'s influence which seems to have affected its findings although the researchers promised not to undertake a commentary on the case. For example, the theoretical side of the commissioned study across Europe and beyond seems to have relied on the phrase *'relating to...'* appearing in Art 2(a) of Directive 95/46/EC to define *personal data.* Accordingly, the research revealed that *personal data* has two possible meanings: one that gravitates around the identification of an individual and the other simply requires an individual's

[341] Ibid, para 30.
[342] Room, S., 'Does *Lindqvist* reveal a Need for a *De Minimis* Principle in Directive 95/46/EC?', LL.M Thesis, Queen Mary University of London, 2004, p.39.
[343] Ibid, pp.38-39.
[344] [2003]UKHL 53; [2003]3WLR 1137.
[345] Room, note 342, supra.
[346] Booth, S *et al.*, 'What are "Personal Data"?' A Study conducted for the UK Information Commissioner, University of Sheffield, 2004.

interest to be engaged.[347] The former is made difficult by the possibility of not only 'direct' but also 'indirect' identification.[348] 'Indirect' identification, where an individual could be identified from the data or the data and other data, can only be made workable by a concept of reasonableness, as in Recital 26, but conceptually it threatens the possibility of anonymsing or pseudonymsing data effectively to remove it from *personal data*.[349] As to the second limb of interpretation, data being personal by simply concerning an individual, makes almost all data (potentially) fall within the ambit of the Directive, moreover, it prompts extraordinary difficult questions about how such data could be prospectively defined.[350] The research findings revealed that this interpretation, however, is more in line with the relationship between data and the construction of personal identity as found in the sociological and psychological literature.[351] In this way the inclusion of the way an individual thinks about the data in the definition of *personal data* is important for such a definition.[352] Indeed, the Directive allows for the inclusion of certain data as *personal data* simply because the data subject believes it to be so.[353] Undoubtedly this yardstick for defining personal data by looking into what a data subject thinks or believes to be so is too broad and is likely to cause more difficulties to implement in practice. This is because, being a subjective criterion to be determined by reference to every individual on a case to case basis, it will make the law more uncertain and confusing until a data subject speaks out his or her mind as to what he or she believes the information to constitute *personal data* or not. It is also important to point out the empirical side of the Commissioner's research study. The latter was conducted across data protection authorities in Europe and outside. The study makes two key findings:-

> 'Between the jurisdictions surveyed there is confidence in understanding the terms found in the Directive, demonstrated by a lack of need for definition or by a lack of difficulty in defining or interpreting the terms. There is a large degree of similarity in defining "personal data", with consistency in the use of terminology. Despite the "on paper" similarity of definitions covered, Data Protection Authorities demonstrate a remarkable lack of consistency in their

[347] Ibid, p.7, para 15.
[348] Ibid.
[349] Ibid.
[350] Ibid, para 16.
[351] Ibid.
[352] Ibid.
[353] Ibid.

> approaches to the classification of data types as "personal data". These divergences in approach are to be found both within and outside the EU."[354]

However, despite the divergences revealed by the UK Information Commissioner's research study in the above paragraph, the broad interpretation of the term *personal data* seems to be mostly preferred by the Data Protection Authorities in Europe (including UK Information Commissioner).[355] This observation is well captured by the Article 29 Working Party (which is widely constituted by the Data Protection Authorities) in the aftermath of *Durant*.[356] The first point to note is that the Article 29 Working Party cautions about overstretching or unduly restricting the definition of personal data from the one intended by the Directive 95/46/EC.[357] In other words, the Article 29 Working Party says in assigning meaning to the term *personal data* a broad approach should be preferred to a *too* broad or narrow interpretation. To ensure the interpretation stays within the ambit of a broad approach, the Article 29 Working Party opined

---

354 Ibid, p.9. para 27.

355 It is worth noting that immediately after *Durant* the UK Information Commissioner's Office issued a new Guideline, 'The "Durant" Case and Its Impact on the Interpretation of the Data Protection Act 1998', http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf last visited 03/11/2011. In such Guideline the Information Commissioner purported to comply with the interpretation of *personal data* as offered in the *Durant* case: demonstrated by citation of the case in the Guideline's introduction as well as frequent reference to the principles developed by the Court in that case. For example, at some point in the Guideline (p.3) the Commissioner made it clear that information that has as its focus something other than the individual will not be *personal data* and gave an illustration of information that focuses on a property (e.g. a structural survey) is not personal data nor is information about the performance of an office department or a branch of a chain of stores. Yet at p.4 of the Guideline the Commissioner provided two other illustrations in which though an individual appears not to be directly identified or to be central of the processing, such information qualified as *personal data*. The first of such illustrations is about a house. He asserts that where information on individual appears in an evaluation report where this was being used in order to determine the assets of a particular individual in a matrimonial dispute that will constitute *personal data*. The other example involves the details of a car photographed by a speed camera where those details are used to direct notice of intention to prosecute to the registered keeper of the vehicle. Arguably these illustrations have exceeded the ambit of *Durant* for attempting to broaden the definition of *personal data* which neither fits into the Court's biographical significance test nor the focus test. The Commissioner's efforts to depart from *Durant* are also demonstrated in the introduction of his Guideline (p.1) where he categorically says, 'this guidance will shortly be replaced by more general guidance on the scope of "personal data". This new guidance will be informed by the work of the Article 29 Working Party subgroup that is currently looking into the meaning of "personal data"'. It is submitted that the Commissioner was definitely sure that the narrow interpretation in *Durant* would not be favoured by the Article 29 Working Party presumably because of the wider criticisms from various Data Protection Authorities across Europe (which largely compose the Article 29 Working Party) as well as criticisms from academics over the restrictive meaning in *Durant*. In fact after the Article 29 Working Party issued its opinion on *personal data* as discussed subsequently in this thesis, the UK Information Commissioner's Office issued a new guidance mixing both the Article 29 Working Party's Opinion as well as the 'biographical significance' and 'focus' tests in *Durant* attempting to balance the two, see Marchini, R., 'United Kingdom Changes in Case Law Update, Part 1: Reconciling the Irreconcilable-the *Harcup* Information Tribunal Decision pits *Durant* against ICO Guidance', World Data Protection Report, March, 2008, p.2, http://www.dechert.com/files/Publication/4fd53e66-e365-4dc5-a5bc-7955b94c0608/Presentation/PublicationAttachment/97858baa-c409-4682-91a9-7b8dec888831/Reconciling%20the%20Irreconcilable%20-%20The%20Harcup%20Information%20Tribunal%20Decision%20Pits%20Durant%20Ag.pdf last visited 04/11/2011.

356 Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data', 01248/07/EN, WP136, (adopted on 20th June 2007).

357 Ibid, p.5.

that in order to consider that the data *'relate to'* an individual, a 'content' element or a 'purpose' element or a 'result' element should be present.[358] The use of the word 'or' after each criterion makes the assessment not cumulative but rather each criterion should be independently assessed. Thus, the 'content' element is present in those cases where information is given about a particular person, regardless of any purpose on the side of the *data controller* or of a third party, or the impact of the information on *the data subject*.[359] Under this criterion therefore information *'relates to'* a person when it is 'about' that person, and this has to be assessed in the light of all circumstances surrounding the case.[360] Illustrating this point, the Article 29 Working Party says, for example, the results of medical analysis clearly relates to the patient, or the information contained in a company's folder under the name of certain client clearly relates to him, etc. As to a 'purpose' element, this is considered to exist when data is used or is likely to be used, taking into account all the circumstances surrounding a precise case, with the 'purpose' to evaluate, treat in a certain way or influence the status or behaviour of an individual.[361] When this is ascertained then data is said to *'relate to'* an individual. A 'result' element exists in situations where the use of data is likely to have an impact on a certain person's rights and interests taking into account all circumstances surrounding the precise case.[362] The degree of impact is immaterial.[363] It is only sufficient if the individual may be treated differently from other persons as a result of the processing of personal data.[364] All what it means from a 'content' element, a 'purpose' element or a 'result' element is that the same piece of data could feasibly relate to different individuals.[365] The same information may relate to individual A because of the 'content' element (the data is clearly about A), and to B because of the 'purpose' element (it will be used in order to treat B in a certain way), and to C because of the 'result' element (it is likely to have an impact on the rights and interests of C).[366] Commentators have similarly criticised the Article 29 Working Party's interpretation of *personal data* as problematic. Applying a 'content' element, a 'purpose' element and a 'result' element in *Durant*, Marchini and Tebbut argue that, the 'content' element is not fulfilled because the Court found that the information complained by *Durant* was about his

---

358 Ibid, p.10.
359 Ibid.
360 Ibid.
361 Ibid.
362 Ibid, p.11.
363 Ibid.
364 Ibid.
365 Marchini, R and Tebbut, K., 'European Data Protection Authorities Provide New Guidance on "Personal Data,"' A Legal Update from Dechert's Data Protection and Privacy Group, July, 2007, No.3, p.2, http://www.dechert.com/files/Publication/2a0df877-51ec-4a46-a96d-6d193b4dfb20/Presentation/PublicationAttachment/d01f7677-2d9d-464e-a20e-6d96f03477bb/DPP_Update3_%207-07.pdf, last visited 03/11/2011.
366 Ibid.

complaint but not about himself.[367] They also argue that *Durant's* complaint would fair under the 'purpose' element if the correspondences between FSA and Barclays (or internal FSA minutes) were used by FSA to determine how they would treat *Durant*.[368] But that was not the case as the FSA processed the information for the purpose of investigating *Durant's* complaints and, arguably, he was mentioned in the internal documents and correspondence at issue only as instigator of the complaint.[369] As regard the 'result' element, this would be fulfilled only if the outcome of the complaint lodged by *Durant* would possibly have had such impact.[370] The authors argue that this may also not be fulfilled because not all rights and interests that should be taken into consideration, but only those which impact the purpose of the Directive; namely the individual's right to privacy(a consideration which the UK Court in *Durant* had firmly in mind).[371]

Worthy important to mention is the fact that some commentators have attributed the *Durant* case narrow interpretation to the law itself and not its interpretation. For example, McCullagh argues that the definition of personal data in the UK legislation is narrower than the Directive 95/46/EC as the UK law refers to 'identified' whereas the Directive refers to 'identifiable' and would potentially exclude the processing of a CCTV image where a specific individual could not be identified by name from the image.[372] She notes that *Durant* did not consider the issue of 'identifiability' of an individual in the definition of personal data set out in section 1(1) of the UK Data Protection Act 1998, instead, the Court concentrated on the meaning of 'relate to' in the definition.[373] In contrast, Lindsay does not see if 'identifiability' was really at issue. He notes that 'identifiability' was not an issue because the information in the manual files essentially concerned letters of complaint written by *Durant* and material generated in response to those complaints.[374] Furthermore and in contrast to McCullagh, Rempell argues that in the UK Data Protection Act 1998 *personal data* definition is consistent with the Directive 95/46/EC requirements only that the English Court of Appeal flawed its interpretation.[375] This view seems to be highly convincing

---

[367] Ibid, p.4
[368] Ibid.
[369] Ibid.
[370] Ibid.
[371] Ibid.
[372] McCullagh, K., 'A Study of Data Protection: Harmonisation or Confusion?', 21st Annual British & Irish Law, Education and Technology Association (BILETA) Conference 'Globalisation and Harmonisation in Technology Law' Malta, April, 2006, p.7.
[373] Ibid, p.9.
[374] Lindsay, D., 'Misunderstanding "Personal Information": Durant v Financial Services Authority', Privacy Law & Policy Reporter, 2004, Vol.10, No.10, http://www.austlii.edu.au/au/journals/PLPR/2004/13.html, last visited 03/11/2011.
[375] Rempell, S., 'Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas', Florida Journal of International Law, 2006, Vol.18, pp. 807-842, at p.823.

for two reasons. First, up to the point *Durant* was decided, criticisms about the scope and limit of the concept of *personal data* under the UK Data Protection Act 1998 were virtually absent. This is dispite the fact that the UK law uses only the term 'identified' as against the Directive 95/46/EC which embraces both two concepts 'identified' and 'identifiable' in the definition of *personal data*. Second, with exception of few commentators, majority of them are of the view that *Durant* only restrictively interpreted the term *personal data*. This is also the case with the Article 29 Working Party which attempted to clarify the meaning of the term *personal data* but did not address itself to the various ways in which Art 2(a) of Directive 95/46/EC defining *personal data* has been transposed in the domestic legislation of the EU member states.

Three submissions can be made in winding up this part. First, in the absence of interpretation from the European Court of Justice (ECJ) which is more likely to be broader than *Durant,* there are absolutely thin chances that UK will change its judicial interpretation of the term *personal data*. This is because in *William Smith v Lloyd TBS Bank plc*[376] the UK High Court, Chancery Division affirmed *Durant* presumably due to the common law doctrine of precedent which requires subordinate courts in a judicial hierarchy to follow principles set down by superior courts.[377] Similarly the Court of Appeal had itself reiterated its stance taken in *Durant* in *David Paul Johnson v the Medical Defence Union*.[378] It is important to point out that the opportunity to correct *Durant* disappeared in 2008 following the House of Lords' (UK Supreme Court) decision in *Common Services Agency v Scottish Information Commissioner*.[379] Although this decision did not strictly uphold *Durant* its option to leave it untouched while such an opportunity to review it was available suggests that the Lords too support *Durant* as correct position of the law.[380] This approach may partly reflect the conservative attitude of the UK judiciary towards protection of personal data as

---

376 [2005]EWHC 246(Ch).

377 See, e.g., Williams, G., Learning the Law, 11th Edition, Universal Law Publishing Co. Pvt. Ltd under special arrangement with Sweet & Maxwell, New Delhi, 2002, p.84. Note that in UK the Court of Appeal is higher than the High Court in the ranks of courts in that case it is bound to follow all principles made by the UK Court of Appeal.

378 [2007]EWCA Civ 262; see also, Jagessar, U and Sedgwick, V., 'When is Personal Data not "Personal Data"-The Impact of Durant v. FSA.', Computer Law & Security Report, 2005, Vol. 21, No. 6, pp.505-511, at pp. 508-510; Watts, M., 'Information, Data and Personal Data-Reflections on *Durant v. Financial Services Authority*', Computer Law & Security Report, 2006, Vol. 22, No.4, pp.320-325, at pp. 520-521; Hodgkinson, D and Wright, T., 'Johnson v The MDU: "Processing" under the DPA', e-Commerce Law & policy, 2007, Vol.9, No.5, pp.1-4, http://www.pillsburylaw.com/siteFiles/Publications/64764B0AFAAE3CF5705A30956A17A860.pdf last visited 5/11/2011; Chalton, S., 'The Court of Appeal's Interpretation of "Personal Data" in Durant v. FSA-a Welcome Clarification, or a Cat amongst the Data Protection Pigeons?', Computer Law & Security Report, 2004, Vol.20, No.3, pp. 175-181; Turle, M., 'Durant v FSA-Court of appeal's Radical Judgment on the Data Protection Act', Computer Law & Security Report, 2004, Vol. 20, No.2, pp.133-136.

379 [2008]UKHL 47.

380 See, e.g. Church, P and Cumbley, R., 'What is Personal Data? The House of Lords identifies the Issues-Common Services Agency v. Scottish Information Commissioner[2008]UKHL 47', Computer Law & Security Report, 2008, Vol. 24, No. 6, pp. 565-567, at p. 566; see also, Burdon and Telford, p. 5, note 312, supra.

claimed by Room.[381] Second, there are little chances for the restrictive interpretation of *personal data* to be given by other courts in Europe, probably because of preventing further risk of disharmony between UK data protection law and the laws of other EU Member States.[382] Third, despite the fact that *Durant* restrictive interpretation of the term *personal data* has accentuated the challenges facing EU Member States in their efforts to achieve harmonisation of data protection, that fact alone, cannot hamper such efforts to harmonise data protection laws, policies and practices across EU. Two reasons support this view. First, since *Durant* was decided, there is no any EU country that has attempted to offer narrow interpretation of the term *personal data* as revenge to UK for providing less protection to its citizen whose personal data have been processed in UK. Second, efforts have been exerted towards achieving a broad interpretation of the term *personal data*. Undoubtedly, the success of these efforts may only be clarified by the European Court of Justice through reference from national courts of the EU Member States.

2.3 Philosophical and Legal Theories of Privacy

The recognition of privacy as a concept worthy of distinct treatment by law is a relatively recent development and dates back to a seminal article by two Harvard academics at the end of the nineteenth century.[383] Subsequently, theories of privacy began to emerge in different disciplines such as philosophy, law, sociology, psychology, science, informatics, political science, medicine, ethics, etc. There is consensus among commentators across these disciplines that privacy is a notoriously difficult concept to define as such there is no single, widely and commonly accepted, comprehensive theory of privacy. This difficulty has been expressed in scholarly writings in a number of ways. Solove summarises the sentiments as underscored by some influential scholars in the following paragraph:-

> 'Time and again philosophers, legal theorists and jurists have lamented the great difficulty in reaching a satisfying conception of privacy. Arthur Miller has declared that privacy is difficult to define because it is exasperatingly vague and evanescent. According to Julie Inness, the legal and philosophical discourse of privacy is in a state of chaos. Alan Westin has stated that few values so fundamental to society as privacy have been so undefined in social theory...William Beaney has noted that even the most strenuous advocate of a

[381] Room, note 343, supra.
[382] Chalton, p.179, note 378, supra.
[383] Gunasekara, G., 'The "Final" Privacy Frontier? Regulating Trans-Border Data Flows', International Journal of Law and Information Technology, 2007, Vol.17, No.2, pp. 142-179, at p.150.

> right to privacy must confess that there are serious problems of defining the essence and scope of this right. Privacy has a protean capacity to be all things to all lawyers. Tom Gerety has observed. According Robert Post privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.'[384]

The difficulty to define *privacy* in the preceding paragraph has been explained based on a number of reasons. For example, Westin contends that no durable definition of privacy is possible because privacy issues are fundamentally matters of values, interests and power.[385] Yet, Moore notes that privacy is a difficult notion to define in part because rituals of association and disassociation are cultural and specific-relative.[386] He illustrates that opening a door without knocking might be considered a serious privacy violation in one culture and yet permitted in another.[387] Liver associates the difficulty to define the notion of privacy to the difficulty of defining allied values such as liberty and equality.[388] She contends that it is hard to define privacy because of the absence of a set of necessary and sufficient conditions which would enable us to identify privacy and distinguish it from allied concepts suggesting that the fuzziness of our concepts of liberty, equality and rights may, themselves, explain why the boundaries of privacy are hard to fix.[389] Liver's reasoning implies that privacy is derivative of liberty and equality. Gutwirth posits that privacy is a difficult concept to define because it is not a tangible object that can easily be corralled into a confined definition.[390] While taken together these explanations have merit, it is important to underline that other factors which have made the notion of privacy difficult to define precisely include, for example, various backgrounds of disciplines where the theorists belong. Accordingly, a legal definition of the notion of privacy becomes significantly different from the one in the medical field, etc. Also the many facets of privacy compounded by the development of modern technologies have increased the difficulty with which the notion of

---

384 Solove, D.J, 'Conceptualising Privacy', California Law Review, 2002, Vol. 90, No.4, pp. 1087-1156, at pp.1088-1089.
385 Westin, A., 'Privacy in America: An Historical and Socio-Political Analysis', National Privacy and Public Policy Symposium, Hartford, 1995, cited in Deighton, J., 'The Right to be Let Alone', Journal of Interactive Marketing, 1998, Vol.12, N0.2, pp.2-4, at p.2.
386 Moore, A., 'Defining Privacy', Journal of Social Philosophy, 2008, Vol. 39, No.3, pp.411-428, at p.411.
387 Ibid.
388 Liver, A., On Privacy, Forthcoming from Routledge (November 2011), p.3, http://www.alever.net/DOCS/On_privacy_intro.pdf last visited 12/11/2011.
389 Ibid.
390 Gutwirth, p.29, note 30, supra.

privacy can be defined. In connection to this, Gutwirth raises a number of questions though he proposes not to answer them in his book:-

> 'The issue of computerised processing of personal data seems to monopolize the interpretation of privacy. Nowadays, privacy is often defined as the control of individuals over what happens with their personal information. Privacy is purely turned into a check on the gathering, linking, processing, distribution and communication of data on individuals. It merely sets the limits within which these daunting activities can take place. The question arises whether such a limited perspective is not problematic. Does it allow us to say something about the importance of privacy in our society? Does it allow us to reflect on privacy's role as a core condition for a democratic constitutional state? Does this perspective allow us to tap into privacy's rich history? Does this limited perspective create the risk that certain key questions will not be asked, allowing for the domination of an eroded concept of privacy? Doesn't one run the risk of building on incomplete, skewed and tendentious preconceived notions? And, does one have to look for a –deliberate or unintentional-hidden agenda?... Is there no discrepancy between privacy invoked as a buffer against electronic personal data processing and privacy referred to by countless fundamental national and international norms? Doesn't it raise suspicion that the loud and omnipresent privacy discourse-yes, even privacy cult-emerges at a time when the practice and technology of transparency, behavioural control and influencing is at its zenith of accuracy, de facto reducing privacy to very little indeed? And is this suspicion not further fed by politicians, legal scholars, business and banking officials using the media to pay lip service to the privacy cult? Or is it because "privacy laws" in fact allow for the wholesale processing of personal data? Does this not again raise the question to what extent the privacy discourse and the new legislation it entails are really aimed at protecting privacy, or whether they are aimed at providing the legal endorsement for the violation of privacy at the service of other interests?'[391]

[391] Gutwirth, pp.2-3, note 30, supra.

Apart from the technological push, *privacy* continues to evolve time and again across different cultures because of the socio-economic and political developments. These transformations have added complication in defining privacy because previously the definitions of privacy were postulated with reference to Western cultures rich in individualistic perceptions. The case in point are the individualism-determinism theories discussed in chapter one. However other cultures like those in Japan, China, and Islamic states have made attempts to trace and locate privacy in their respective cultures in the context of prevailing socio-economic and political developments.

Lack of precise definition of *privacy* is not only noticeable in the privacy theories but also in international and regional instruments as well as national legislation protecting privacy. In the latter case, usually no such definitions are offered. Courts, through case law, have too strived to define the concept of privacy in vain as in most cases such case law definitions go back to one or more theories of privacy which none of them is so far universally accepted as conclusive. Bygrave argues that lack of a precise definition of the concept of privacy in data protection laws should not necessarily be considered as a weakness in the data protection laws rather as a room for flexibility in their implementation.[392] Also the vagueness of the privacy concept (and thereby data protection laws) helps to assimilate and address a range of fears related to increasingly intrusive data-processing practices.[393] Moreover, letting in a large concept like privacy undefined in data privacy laws helps to offset an equally large rhetorical counter-claim: freedom of inquiry, the right to know, liberty of the press and so on.[394] Yet, there are some disadvantages for failure to define privacy in the data protection laws. Such a failure has a cost in so far as it detracts from the capacity of those laws for prescriptive guidance.[395] Also, it perpetuates the vulnerability of the privacy concept to the criticisms that it is incapable of definition, has no independent, coherent meaning and should be subsumed by other concepts.[396]

Despite the pitfalls explained above in defining *privacy*, several attempts have been made to define it. Before examining these theories i.e. their main assumptions, strength and weaknesses, it is worth to highlight four important points that should provide guidance in assessing them. First, none of those privacy theories should be considered more superior or conclusive than the other. This is owing to the fact that it is difficult to resolve conclusively the privacy debate on definition

[392] Bygrave, p.278, note 277, supra.
[393] Ibid.
[394] Ibid.
[395] Ibid.
[396] Ibid.

of privacy because such debate rests to a considerable extent on intuitive assessments of how privacy should commonly be understood.[397] Gutwirth observes that the dispute over privacy's definition cannot be settled leaving the question why a slew of intelligent and sophisticated legal scholars have tried, and continue to try, to come up with a precise description and a conclusive definition of the term.[398] Consistent with this view, Liver argues that despite the difficulty in defining privacy, we will need to get behind such concept, and give it more shape and definition if we are to make progress in thinking about it.[399] Second, the theories of privacy discussed below are either broad, narrow or slide back and forth between the two ends of the spectrum. Third, whether broad, narrow or in between the two ends, privacy theories are either normative or non-normative/descriptive.[400] [401] The former makes references to moral obligations or claims while the latter refers to a state or condition where privacy obtains.[402] Fourth, the privacy debate carries with it various dangers, including underplaying the multidimensional character of privacy and overlooking the fact that law and policy do not always need to operate with precise definitions of values.[403]

There are several theories of privacy. While such theories seem to be different, they overlap and share common features. Because of this, commentators analyse these theories in their respective common groups. This approach helps to maintain a clear focus in analysis and facilitate their understanding. Yet, there are no agreed classifications for these theories. For example, Bygrave groups such definitions of privacy into four classes: information control, non-interference, limited accessibility and intimacy.[404] Tavani classifies privacy theories into four groups as Bygrave but he uses somewhat different nomenclature: noninstrusion, seclusion, limitation, and control theories.[405] Equally important to note is the fact that although the two sets of classifications are equal in number, they are different in contents. For example, while Bygrave's classification includes intimacy Tavani's excludes it. Also, Bygrave's inclusion of non-interference can be equated with Tavani's nonintrusion. However it is difficult to see the fitting of Tavani's seclusion in Bygrave's classification. Similar to Bygrave and Tavani, Davis maintains a four number classification of privacy theories: concepts of leaving alone, control, limited access and

[397] Bygrave, note 392, supra.
[398] Gutwirth, p. 34, note 30, supra.
[399] Liver, note 388, supra.
[400] Tavani, H.T., 'Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy', METAPHILOSOPHY, 2007, Vol.38, No.1, pp. 1-22, at p.3.
[401] Moore, pp.412-413, note 386, supra.
[402] Ibid.
[403] Bygrave, note 392, supra.
[404] Ibid, pp. 279-281.
[405] Tavani, p.4, note 400, supra.

possession of information.[406] However, they are somewhat overlapping with those classifications by Bygrave and Tavani. Yet, Davis' classification differs from Bygrave's and Tavani's in that the former includes possession of information theories while the latter do not. In contrast to the four classifications, Whitley classifies privacy theories into three groups: privacy as no access to the person or the personal ream, privacy as control over personal information and privacy from judgement or scrutiny by others.[407] While the first two categories of Whitley's classification of privacy theories fit into Bygrave's and Tavani's, the latter falls outside those theories. Yet, Solove groups privacy theories into six: the right to be let alone, limited access to the self, secrecy, control over personal information, personhood and intimacy.[408] Solove's classification overlaps. For example, the theories on secrecy and personhood transcend the ones on the right to be let alone and limited access to the self. This overlapping reduces his classification into four similar classes as Bygrave. The six classification of privacy theories are also adopted by the New Zealand's Law Commission which groups these theories as reductionism, the right to be let alone, limited access to the self, concealment or control of personal information, personhood, intimacy and pragmatism.[409] As can be noted, the New Zealand's classification of the privacy theories follows closely Solove's. There are however markedly differences. The New Zealand's classification omits the theories on secrecy but adds the pragmatism which is Solove's own theory. Since the above classifications possess some common features, of course with some differences too, the six classifications of the privacy theories which combine elements of the above are adopted here for purpose of this thesis. These include: information control, non-interference, limited accessibility, reductionism, intimacy and pragmatism.

2.3.1 Information Control Theory

This theory has two main assumptions: first, an individual has power, whether direct or indirect over his or her personal information *vis-a-vis* the data controllers or data processors, second, but in alternative to the first assumption, an individual may influence whether directly or indirectly processing of personal information about him or her by data controllers or data processors. In effect, however, *power* and *influence* may be considered to be one and the same thing because the exercise of *power* automatically involves elements of *influence* and *vice versa*.

---

406 Davis, S., 'Is there a Right to Privacy?', Pacific Philosophical Quarterly, 2009, Vol. 90, No.4, pp.450-475, at p. 451.
407 Whitley, p. 155, note 308, supra.
408 Solove, pp.1092, 1094, 1199, note 384, supra.
409 New Zealand's Law Commission, 'Privacy: Concepts and Issues, Review of the Law of Privacy Stage 1', Study Paper 19, Wellington, 2008, pp.31-40,
http://www.lawcom.govt.nz/sites/default/files/publications/2008/02/Publication_129_390_SP19.pdf last visited 13/11/2011.

There are many variants of information control theory. However Westin's classical theory has been widely cited by commentators because of the great influence it exerts in the privacy discourse. Perhaps because of this influence, sometimes the information control theory has been reduced to Western's definition: 'privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'[410] While this approach features prominently in privacy literature as it captures the essence of the entire theory, it tends to infuse and undermine other variants of the information control theory by subjecting them into Westin's. Margulis argues that the variation in specific definitions reflects how the terms and the relationships among terms, in the formal definition, were interpreted within those definitions.[411] Accordingly, he notes limitations of his own variant which states, 'privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability'.[412] Also important to note here is the fact that with the exception of other variants, Westin's variant of information control theory defines privacy in terms of both individual and groups. This definition may have significant implication in such societies where groups are dominant over the individual. The other variants of information control theory are summarised by Tavani in the following paragraph:-

> 'According to Fried, privacy "is not simply an absence of information about us in the minds of others, rather it is the control over information we have about ourselves"(1990,54). Miller embraces a version of the control theory when he describes privacy as "the individual's ability to control the circulation of information relating to him" (1971, 25). A version of the control theory is also endorsed by Westin...And Rachels appeals to a version of the control theory of privacy in his remarks concerning the connection between "our ability to control who has access to information about us and our ability to create and maintain different sorts of relationships"(1995, 297).'[413]

The information control theory has also manifested itself in terms of concealment. An example of information concealment theorists is Posner who, while avoids defining privacy, he finds that

---

[410] Westin, A.F, Privacy and Freedom, Atheneum Press, New York, 1967, p.7.
[411] Margulis, S.T., 'Privacy as a Social Issue and Behavioral Concept', Journal of Social Issue, 2003, Vol.59, No.2, pp.24-261, at p.245.
[412] Ibid.
[413] Tavani, p.7, note 400, supra.

one aspect of privacy is the withholding or concealment of information.[414] Equally important to note is the fact that the information control theory entails some elements of ownership rights over individual's personal information. Parent provides a good example here. He defines privacy as, '...the condition of not having undocumented personal knowledge about one possessed by others.'[415]

Critics of the information control theory have raised a number of objections. First, they assert that the theory wrongly assumes that one looses privacy when he or she no longer has control over his or her personal information. Conversely, the critics view that there can be a loss of control without a loss of privacy and a loss of privacy without a loss of control.[416] In other words, the information control theorists are criticised here because of lack of clarity as to which kinds of personal information one can expect to have control over and how much control one can expect to have over one's personal information.[417] Yet, this criticism has been countered by Shoemaker who asserts that such criticism seems to be unfair given that a control theorist could easily say that one's privacy ranges over a specific domain of generally unrevealed information, and one has privacy to the extent one exercises control over access to that domain.[418] Thus, if there is simply no unrevealed personal information left over which one could exercise control, one would have no privacy either.[419] Nevertheless, the problem of vagueness still hovers over the control theory as it needs clearly to address what specifically counts as the relevant zone of

---

414 Posner, R.A., 'The Right of Privacy', Georgia Law Review, 1978, Vol. 12, No.3, pp.193-422, at p. 193.

415 Parent, W.A., 'Privacy, Morality, and the Law', Philosophy & Public Affairs, 1983, Vol.12, No.4, pp.269-288, at p. 269.

416 Davis, p.452, note 406, supra.

417 Tavani, pp.7-8, note 400, supra; see also Ritchie, D., 'Is it Possible to define "Privacies" within the Law? Reflections on the "Securitisations" Debate and the Interception of Communications', International Review of Law, Computers & Technology, 2009, Vol.23, Nos.1-2, pp.25-34, at p. 30 where Ritchie provides an example of a person walking down a street covered by closed circuit television(CCTV) who has no say in how much information will be stored or communicated to others yet in another sense it can be argued that he or she has accepted the surveillance by not choosing to avoid that particular street. However this latter argument of individual's right of choice to avoid CCTV is sometimes problematic especially where such alternatives do not exist for one to opt, let say for example, a particular service which one is in need is only available along a particular street or place covered by CCTV; Whitley, note 407, supra, in explaining the problem of the information control theory in an online environment and particularly in terms of the extent an individual can exercise control over his or her personal information, makes the following observations: 'control...is seen as something that occurs at the start of a disclosure process and privacy control is seen solely in terms of limiting what personal data is made available to others. In practice, however, this is a rather partial view of how personal data is disclosed and shared by others. It is increasingly common for individuals to register with various online services and disclose data about themselves (name, email address, etc.). This data is then stored in enterprise databases for significant periods of time and may be shared with other parts of the enterprise or selected third party organisations. Whilst in earlier times control over personal data may have been best undertaken by preventing the data from being disclosed, in an internet enabled society it is increasingly important to understand how disclosed data is being used and reused and what can be done to control this further use and reuse.'

418 Shoemaker, D.W., 'Self-Exposure and Exposure of the Self: Informational Privacy and the Presentation of Identity', Ethics and Information Technology, 2010, Vol.12, No.1, pp.3-15, at p.4.

419 Ibid.

personal information(and why) and also the extent of control required.[420]Second, the information control theory and especially Westin's variant has been criticised for being narrow in context. Westin's definition of privacy presupposes that if there is a loss of privacy, then something has been communicated.[421] Yet, not all losses of privacy involve communication.[422] One of such instances where there is loss of privacy without communication of information is illustrated by Davis by assuming himself to be in his room naked and someone pees into the window.[423] Here there is loss of privacy as the Peeping Tom has come to know what he looks like without his clothes yet nothing has been communicated to the Peeping Tom.[424] Third, property rights have also raised many objections from critics of the information control theory. Moore argues that if property rights and privacy rights are both essentially about control, then maybe privacy rights are simply a special form of property rights.[425]Consistent with this view Solove observes:-

> 'Information can be easily transmitted, and once known by others, cannot be eradicated from their minds. Unlike physical objects, information can be possessed simultaneously in the minds of millions. This is why intellectual property law protects tangible expressions of ideas rather than underlying ideas themselves. The complexity of personal information is that it is both an expression of the self as well as a set of facts, a historical record of one's behaviour....Personal information is often formed in relationships with others, with all parties having some claim to that information.'[426]

To put it differently, property right concepts present significant challenges for being extended to information privacy. These challenges range from concepts to the principles of ownership of physical properties. Fourth, the information control theory has been challenged for its failure to make distinction between potential and actual violations of privacy.[427] Elgesem argues that by

---

[420] Ibid.
[421] Davis, note 416, supra.
[422] Ibid.
[423] Ibid.
[424] Ibid.
[425] Moore, p.418, note 386, supra.
[426] Solove, p.1113, note 384, supra. For more discussion about protection of privacy as property rights see e.g., Butchner, B and Kang, J., 'Privacy in Atlantis', Harvard Journal of Law & Technology, 2004, Vol. 18, No.1, pp.229-267 where the 'Economist' raises arguments in favour of protection of personal information as any other commodity/tangible property; Litman, J., 'Information Privacy/Information Property', Stanford Law Review, 2000, Vol. 52, pp.1283-1313; Prins, J.E.J., 'The Propertization of Personal Data and Identities', Electronic Journal of Comparative Law, 2004, Vol.8, No.3, pp.1-7.
[427] Elgesem, D., 'The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data', Ethics and Information Technology, 1999,

defining privacy as control over personal information, also threats of privacy violations seem to be counted as actual violations of privacy.[428]

Despite the objections raised against the information control theory, it has been viewed to be directly applicable to the issues raised by the data-processing practices of organisations.[429] The information control theory also harmonises fairly well with, and builds upon, many of the basic rules of data protection law, particularly those rules that enable persons to participate in, and influence, the processing of information about them.[430] Furthermore the theory lends the concept of privacy considerable normative force, as it allows privacy advocates tapping into the dynamic ethical undercurrent associated with the idea of self-determination.[431]

2.3.2 Non-interference Theory

The non-interference theory or noninstrusion or seclusion, has its roots in the seminal article of Samuel Warren and Louis Brandeis-'the Right to be let Alone'. It is unsurprising that because of this background some commentators such as Solove simply refer to this theory as the right to be let alone.[432] Yet, this reference of the non-interference theory to the right to be let alone is too simplistic because it leaves out other variants of the non-interference theory which do not specifically refer to the right to be let alone. Thus, reference to non-interference theory is preferred here to simply the right to be let alone.

The main assumption of the non-interference theory is that an individual is considered to be in a state of privacy if and only if he or she is not interfered in any way by any person. Putting this in other way, an individual is considered to have privacy if no one tries to involve in and tries to influence or gain access to his or her personal information. As pointed out, the most prominent variant of the non-interference theory is the right to be let alone. It is widely acknowledged by commentators that the variant of the right to be let alone does not provide either a definition or a coherent conception of privacy.[433] The non-interference theory also contains elements of a number of the other conceptions including limited access to the self, control over personal

---

Vol.1, No.4, pp.283-293, at p. 290; see also Volkman, R., 'Privacy as Life, Liberty, Property', Ethics and Information Technology, 2003, Vol.5, No.4, pp.199-210, at p. 203.

[428] Ibid.

[429] Bygrave, p.279, note 277, supra.

[430] Ibid.

[431] Ibid.

[432] Solove, note 408, supra.

[433] New Zealand's Law Commission, p.32, para 2.7, note 409, supra.

information, and personhood.[434] However, the main criticism against the non-interference theory and concomitantly the right to be let alone comes from Allen who argues that if privacy simply meant 'being let alone', any form of offensive or harmful conduct directed toward another person could be characterised as a violation of personal privacy.[435] More so, a punch in the nose would be a privacy invasion as much as a peep in the bedroom.[436] Tavani has attacked the non-interference theory on two grounds: first, some versions of the nonintrusion theory tend to confuse the condition (or content) of privacy with a right to privacy.[437] He notes this confusion in the variant of Brandeis and Brennan, and second, in defining privacy in terms of being free from intrusion, the nonintrusion theory confuses privacy with liberty.[438] Solove simply criticises the right to be let alone as a rather broad and vague conception of privacy.[439] Another criticism advanced against the right to be let alone is that it fails to distinguish normal ways of human interaction with intrusive ones. Its underlying assumption seems to be that people build their lives individually, and interferences from others are a hindrance at best.[440] Arguably, this is a bit simplistic as people engage voluntarily in interactions and often need the attention of others for a satisfactory life.[441] In practice, however, the right to be let alone often leads authors to the standpoint that any bit of information about you is a privacy concern and in the ideal world no information about you would be collected at all.[442]

Despite the above pitfalls, the non-interference theory and more particularly the right to be let alone has its credit. The article by Warren and Brandeis in which the variant of the right to be let alone is contained was far ahead of its time, and it contained flashes of insight into a more robust theory of privacy.[443] Also, Warren and Brandeis's aim was not to provide a comprehensive conception of privacy but instead to explore the roots of a right to privacy in the common law and explain how such a right could develop.[444]

---

434 Ibid.
435 Allen, A.L., Uneasy Access: Privacy for Women in a Free Society, Rowman & Littlefield, Totowa, NJ, 1988, p.7 cited in Solove, D.J, 'Conceptualising Privacy', California Law Review, 2002, Vol. 90, No.4, pp. 1087-1156, at p.1102.
436 Ibid.
437 Tavani, p.5, note 400, supra.
438 Ibid.
439 Solove, note 435, supra.
440 Heeney, C and Weigand, H., 'Privacy Protection and Communicative Respect', Proceedings of the 8th International Working Conference on the Language-Action Perspective on Communication Modelling(LAP), Tilburg, the Netherlands, 2003, p.3, http://infolab.uvt.nl/research/lap2003/weigand_heeney.pdf last visited 16/11/2011.
441 Ibid.
442 Ibid.
443 Solove, note 435, supra.
444 Ibid.

2.3.3 Limited Accessibility Theory

The limited accessibility theory assumes that one has privacy when access to information about oneself is limited or restricted in certain contexts.[445] In other words, the domain of information to which others have limited or no access simply constitutes one's zone of privacy.[446] Some commentators attribute the rise of the limitation theory to the worries about the information control theory.[447] Yet, this view is doubtful for two reasons. First, some variants of the limitation theory emerged along the same period with the information control theory. Second, the elements of information control theory are still descendible in the limitation theory. Thus, the latter's theory cannot claim to be purely independent from the information control theory.

Under the limitation theory, Gavison's variant appears to be the most dominant. According to her variant, privacy is a limitation of other's access to an individual.[448] She sees this limitation to consist of three elements namely secrecy, anonymity and solitude which work in dependency to each other.[449] Three main objections have been raised against Gavison's variant of limitation theory. First, the definition is too broad: that treating any physical access to a person, or attention paid to a person, or information gained about a person as a loss of privacy robs privacy much of its intuitive meaning.[450] Second, the limitation theory underestimates the role of control or choice that is also required in one's having privacy; it does not take into account that someone who has privacy can choose to grant others access to information about himself or herself, as well as to limit(or even deny) others from access to that information.[451] The theory also seems to imply that one has privacy only to the extent that access to information about oneself is limited or restricted.[452] This in turn implies that the more one's personal information can be withheld (or kept secret) from others, the more privacy one has. Accordingly, in the account of privacy offered in the limitation theory, privacy can easily be confused with secrecy.[453]

However, the limitation theory has been credited on two aspects. First, it correctly recognises the importance of setting up contexts or 'zones' of privacy to limit or restrict others from access to

[445] Tavani, p. 9, note 400, supra.
[446] Shoemaker, note 418, supra.
[447] Ibid.
[448] Gavison, R., 'Privacy and the Limits of the Law', Yale Law Journal, 1980, Vol.89, No.3, pp.421-471, at p.428.
[449] Ibid, pp.433-435.
[450] Wacks, pp.16-18, note 327, supra cited in New Zealand's Law Commission, p.34, note 409, supra.
[451] Tavani, note 445, supra.
[452] Ibid.
[453] Ibid.

one's personal information.[454] Second, it avoids confusing privacy with autonomy, as well as with liberty and solitude.[455]

2.3.4 Reductionism Theory

The reductionism theory does not take privacy as an independent concept. The theorists in this camp assert that privacy is derived from other values or rights such as life, liberty and property rights. It is therefore difficult to isolate privacy from its associated rights. One variant of the reductionism theory is that postulated by Judith Jarvis Thompson. She advances two arguments: that what is commonly described as the right to privacy is a cluster of rights, and that it is unclear what properly belongs to this cluster; and there is no need to find that-which-is-in-common to all rights in the right to privacy cluster and no need to settle disputes about its boundaries.[456] The other variant of reductionism theory was propounded by Davis, who argues:-

> 'If truly fundamental interests are accorded the protection they deserve, no need to champion a right to privacy arises. Invasion of privacy is, in reality, a complex of more fundamental wrongs. Similarly, the individual's interest in privacy itself, however real, is derivative and a state better vouchsafed by protecting more immediate rights.'[457]

The reductionism theory and more specifically Tompson's variant has been criticised for two main grounds. Her definition is too broad for including rights not to be looked at or listened to.[458] Second, even if privacy rights are derivative, they may still form a coherent cluster.[459] Yet, it is important to note that privacy has some sort of connections with other rights. This explains why for example, although the American Constitution lacks express provision on protection of privacy, still the USA Supreme Court as well as the highest courts in various states have been able to derive the right to privacy from other rights expressly provided in the constitution.

---

[454] Ibid.
[455] Ibid.
[456] Thompson, J.J., 'The Right to Privacy', Philosophy and Public Affairs, 1975, Vol.4, No.4, pp.295-314 at pp.305, 306,310.
[457] Davis, F., 'What do We mean by "Right to Privacy"?' San Diego Law Review, 1959, Vol.4, p.20 cited in Moore, p.413, note 386, supra.
[458] New Zealand's Law Commission, para 2.5, note 433, supra
[459] Ibid.

2.3.5 Intimacy Theory

Intimacy theory is relatively unpopular in data protection discourse mainly because intimacy-oriented definitions of privacy are unable to anticipate and capture the process by which detailed personal profiles of individuals are created through combining disparate pieces of ostensibly innocuous information.[460] The main thrust of this theory is that privacy only concerns about the exclusive realms of our personal lives that are 'intimate' or 'sensitive'.[461] Consequently, there is loss of privacy only when 'intimate' or 'sensitive' personal information is disclosed.[462] Fried, one of the theorists under intimacy theory, posits:-

> 'Intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love.'[463]

Fried's variant has been criticised by defining intimate information as information that individuals choose to reveal selectively, without explaining what it is in the particular relationship that makes it intimate.[464] For example, information might be revealed to a psychoanalyst that would never be told to a friend or lover, but this does not make necessarily the patient-psychoanalyst relationship an intimate one.[465] Yet, Inness's variant of intimacy theory appears to be the most influential under this head. According to Inness, privacy is the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions.[466] The strength of this definition is that it has expanded its scope beyond information to access and actions. However, four objections have been raised generally to the intimacy theory. First, privacy may make it possible to develop feelings of trust, love, friendship and caring, but these ends do not form a complete picture of what is commonly considered to be protected by privacy.[467] A good illustration here is financial

---

[460] Bygrave, p.280, note 277, supra.
[461] Ibid.
[462] Inness, J.C., Privacy, Intimacy and Isolation, Oxford University Press, New York, 1992, p.140 cited in Bygrave, note 460, supra.
[463] Fried, C., 'Privacy', Yale Law Journal, 1968, Vol.77, pp.475-493, at pp.484-485.
[464] New Zealand's Law Commission, p.38, para 2.26, note 409, supra.
[465] Ibid; see also, Floridi, L., 'Four Challenges for a Theory of Informational Privacy', Ethics and Information Technology, 2006, Vol.8, No.3, pp.109-119, at p.115-116.
[466] Inness, note 460, supra.
[467] New Zealand's Law Commission, p.39, para 2.28, note 409, supra.

information which is considered private, but is often not regarded as intimate.[468] Second, intimate and/or private matters need not be characterised by love or caring: sexual partners may feel no sense of caring for each other, and relationships between siblings or ex-spouses may be characterised by hatred yet it can still be considered private.[469] Third, intimacy-based conceptions of privacy may also fail to capture many of the concerns about building up detailed personal profiles 'through combining disparate pieces of ostensibly innocuous information', a process that is becoming ever easier with the increasing integration of information systems.[470] Fourth, in some circumstances intimacy, far from being facilitated by privacy, may 'suffocate privacy'.[471] This is particularly the case in small-scale societies where levels of intimacy may be high while levels of privacy are low.[472] The relationship between privacy and intimacy posited by Inness and others appears to apply mainly in modern, individualist and predominantly urban societies.[473]

2.3.6 Pragmatism Theory

Otherwise known as 'problem-solving', the pragmatism theory is relatively the youngest privacy theory. Its proponent is Solove. His postulation appeared for the first time in his renowned article 'Conceptualizing Privacy' (cited in several parts of this chapter) and later his book *Understanding Privacy*[474] which heavily relies on the former and other articles: 'The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure' and 'Taxonomy of Privacy'.[475]

Before putting forward his theory, Solove makes a critical review of the existing theories of privacy which he collectively refers to them as 'traditional accounts of privacy' as opposed to his theory which he refers to it as *A New Theory of Privacy*.[476] Solove's criticisms of the traditional theories of privacy can be summarised in the following paragraph:-

> 'More generally many existing theories of privacy view it as a unitary concept with a uniform value that is unvarying across different situations. I contend that with a few exceptions, traditional accounts of privacy seek to

[468] Ibid.
[469] Ibid, para 2.29.
[470] Ibid, para 2.30.
[471] Ibid, para 2.31.
[472] Ibid.
[473] Ibid.
[474] Solove, D.J., Understanding Privacy, Harvard University Press, Cambridge-Massachusetts/London-England, 2008.
[475] Ibid, p.x.
[476] Ibid, p.8.

> conceptualize it in terms of necessary and sufficient conditions. In other words, most theorists attempt to define privacy by isolating a common denominator in all instances of privacy. I argue that the attempt to locate the "essential" or "core" characteristics of privacy has led to failure.'[477]

Furthermore, Solove faults the traditional theories of privacy for being abstractive.[478] He contends that privacy cannot be conceptualised by searching for a common denominator or essence of privacy.[479] In contrast, he suggests conceptualising privacy in terms of Ludwig Wittgenstein's notion of 'family resemblances'.[480] The latter notion simply means that certain concepts might not share one common characteristic, but might form 'a complicated network of similarities overlapping and criss-crossing.[481] Accordingly, Solove advocates a bottom-up approach instead of a top-down to conceptualising privacy. The bottom-up approach, according to Solove, entails conceptualising privacy based on context-specific situations i.e. examining privacy violations as disruptions of particular practices: interference with peace of mind, intrusion on solitude, or loss of control over facts about oneself.[482] Solove also argues that the value of privacy is also context-specific, in contrast to theories that try to establish an overreaching value of privacy such as protecting dignity or intimacy.[483] Solove views that the value of privacy in particular contexts depends on the purposes of the practices involved, and the importance of those purposes.[484] He argues that privacy should be valued instrumentally as a means of achieving other valuable ends.[485] Reverting to his context-specific approach, he observes that 'the landscape of privacy is constantly changing', particularly as a result of technological developments, and that scholars and judges may be led astray by trying to fit new problems into old conceptions.[486] He remarks:-

> 'We should seek to understand the special circumstances of a particular problem. What practices are being disrupted? In what ways does the

[477] Solove, pp. 1090-1091, note 384, supra.
[478] Ibid, p.1095.
[479] Ibid, pp.1092-1093, 1096, 1098,1099,1126,1154.
[480] Ibid, p.1126.
[481] Ibid.
[482] Ibid, p.1130.
[483] Ibid, p.1143.
[484] Ibid, p.1144-1146.
[485] Ibid.
[486] Ibid, p.1146.

> disruption resemble or differ from other forms of disruption? How does this disruption affect society and social structure?'[487]

Solove's *A New Theory of Privacy* has faced several objections. First, it still allows for large amounts of subjectivity.[488] This is because; society must determine in this problem-based approach what rights privacy trump and which rights trump privacy.[489] Thus coming to a general consensus about the value of privacy compared to other rights in varying situations seems almost impossible; this is because no person holds rights in the same ideological hierarchy.[490] Second, Solove overlooks that at some point someone, most likely the legislature, will have to decide where privacy falls among various rights.[491] Privacy issues looked at through the problem-based approach will be helpful to legislatures tackling this problem but will not be complete; the legislature must rely on some abstract omniscient definition of 'privacy' before the problem-based application can begin.[492] Thus if one attempts to divorce the exercise of 'understanding privacy' from any theory of rights, inevitably, he or she is likely to end right back in the same 'conceptual jungle' he or she were in before.[493] More so, Solove's call to abandon from the traditional theories of privacy is a total misdirection because it attempts to close down the privacy debates which, he himself acknowledges that technological advancement is changing the ways we should look into privacy issues. Third, Solove's theory fails to provide basis for establishing why some harms are privacy violations and others are not.[494] Fourth, the pragmatism theory is in fact a way of conceptualising privacy violations rather than privacy itself.[495] Solove's focus on harms in the form of disruption of specific practices lends itself well to a legal and policy analysis based on the prevention or remedying of harms.[496]

---

[487] Ibid, p.1147.
[488] Foye, S., 'Book Review on Understanding Privacy by Daniel J.Solove', Journal of High Technology Law, 2008-2009, p.4, http://www.law.suffolk.edu/highlights/stuorgs/jhtl/book_reviews/2008_2009/Foye.pdf, last visited 20/11/2011.
[489] Ibid.
[490] Ibid.
[491] Ibid.
[492] Ibid.
[493] Thierer, A., 'Book Review: Solove's Understanding Privacy', The Technology Liberation Front, 2008, p.3, http://techliberation.com/2008/11/08/book-review-soloves-understanding-privacy/ last visited 20/11/2011.
[494] New Zealand's Law Commission, p.41, para 2.37, note 409, supra.
[495] Ibid, para 2.38.
[496] Ibid.

Despite the above objections, Solove's theory of privacy and especially his book *Understanding Privacy* has been credited for providing a deep understanding of the importance of privacy and the erosion of privacy that is currently taking place.[497]

2.4 Choice of Terminologies and Preference of Theory

The present thesis is about protection of personal data in sub-Saharan Africa. However *privacy* concept as opposed to *personal data* or *data protection* features prominently in the thesis. Sometimes one may be tempted to think that the appropriate title of the thesis would have been protection of privacy. Yet, there is no clear line of difference between the terms: *privacy* and *personal data* or *data protection* (see discussion in 2.2). Sometimes the latter may be referring to the former and *vice-versa*. Therefore it is imperative to make clear which reference is employed in this thesis and why as well as which theory is mostly preferred in this thesis.

Both concepts: *privacy* and *personal data* are used in this thesis interchangeably unless specific context excludes the use of the other. Moreover, any collective reference to *privacy and data protection* connotes either the former or latter term. The decision to maintain both terms has taken into account a number of reasons. First, the term *personal data* is relatively new in the privacy discourse in Africa. Scholars and non-scholars trouble to understand what is meant by personal data. During field research it transpired that most of the respondents interviewed had problems of understanding what it meant by the concept of *personal data*. Yet, when a clarification was made using the term *privacy* to refer to what is captured by the concept of *personal data*, the respondents became clear with the terminologies. As pointed out, the problem of conception of *personal data* was not only experienced by the general public but also scholars in academic institutions and beyond. This is not surprising because, data privacy law does not form part of curriculum in most universities in Africa. For example, at the University of South Africa (UNISA), Professor Anneliese Roos admitted during interview that she has to teach other subjects, especially law of succession, despite the fact that her research interests are in data privacy law.[498] This is because such subject is not on offer. The case has also been for Mauritius, where data privacy law is yet part of the curriculum at the University of Mauritius. This is despite the fact that Mauritius has already implemented comprehensive data privacy law. Tanzania has the same experience though with slight difference. The oldest and largest university in Tanzania,

[497] Foye, p.5, note 488, supra.
[498] This is according to the researcher's interview with Professor Anneliase Roos on 28/06/2011 at Pretoria, South Africa.

i.e. the University of Dar es Salaam, does not offer data privacy law in its curriculum. However from 2009, the Open University of Tanzania started to teach data privacy law in its newly established master of law in information technology and telecommunications (LL.M IT & T). It is submitted that data privacy law is an emerging discipline not only in Africa but across the world. However in Europe and America the subject is widely taught in universities as compared to elsewhere. Second, the term *privacy* appears in most national constitutions in African countries and statutory laws. Thus, although it has not become into regular use, it is easier to communicate it than *personal data*. Third, although this thesis is intended for a global audience, it specifically bears legal reformist agenda to the sub-Saharan Africa. Hence it does not seem appropriate to deploy a terminology that is unfamiliar to many in Africa. Fourth, the need to maintain the use of *personal data* has been motivated by the fact that the development of data privacy law in Africa is largely influenced by the European law which uses the term *personal data*. Thus, in order to keep dialogue between the North and South in as far as data privacy policies and regulations are concerned, it is important to have some minimum common understanding of various concepts.

As pointed out in 2.3, privacy theories can largely be reduced into six main groups. Yet none of them should be considered superior or universally acceptable due to the limitations surrounding each. However, despite that, it is still possible to make preference of a particular theory to suit particular context. This approach will not undermine other theories as such preference may not fit other specific contexts in which other theories will do. In this thesis therefore, the limited accessibility theory is preferred because it is in accord with what most data privacy law principles are tailored. As it has been noted, the limited accessibility theory defines privacy in terms of conditions as against rights or claims. The former fits well the data privacy laws which lay down conditions under which personal data processing can be considered to be in compliance with law. However, it must be clearly pointed out that other theories manifest in the data privacy laws as well although with some limitations. For example, the information control theory explains well the requirements of consent as one of the pre-conditions for processing personal data. However, not all processing of personal data must be sanctioned by a data subject. Moreover, with the advancement of modern technologies and particularly the booming of social networks, it has been difficult for data subjects to exercise control over their personal information.

2.5 Conclusion

The discourse of data and privacy law is full of concepts and theories. There are agreements and disagreements with regard to the meanings, scope and ambit of such concepts and theories due to various reasons. However, it is important that some common conceptual understandings are attained. For example, the *Durant's* restrictive interpretation of the term *personal data* has been widely criticised. This indicates that there are possibilities for some concepts to be commonly understood in a particular region or beyond. Yet, in certain cases the common way of understanding concepts is extremely difficult to achieve. This is the case with the term *privacy*. Several theories have been postulated to explain what *privacy* means. However, none of them has precisely defined it in a manner that is agreed by everyone. While conflicting theories over *privacy* continue to emerge with some adverse effects to the value sought to be protected, they have their advantages as well as disadvantages as discussed above.

3. Privacy and Data Protection in International Law

3.1 Introduction

The internationalization of modern privacy and data protection law is a recent phenomenon that has taken place since 1980s. This development which started by European nations owes largely to an attempt by such nations to remove potential obstacles to the flows of information across-nations in order to foster internal market policies and regulations as well as ensuring a high level of its protection.[499] Prior to this internationalization, unilateralism, which means pursuing data protection issues singly and without due regard to other nations, was considered an affair limited within national competency and territoriality. Yet, in certain cases national legislation had/has extra-territorial application.[500] However by 1980s it was vivid that legislative restrictions of transfer of personal data beyond the territory of a particular state were leading to economic barriers and isolation as well as provision of weak protection of personal information. To obviate and address those challenges, bilateral agreements and subsequently harmonization of privacy and data protection policies and legislation regionally and internationally provided new avenues.

This chapter provides an overview of privacy and data protection as it manifests in international law. By 'international law' as used in this context it means that law whether binding or non-binding, negotiated at the supranational bodies and as a result of which its territorial reach goes beyond national sovereignty. Thus the legal and regulatory instruments adopted to govern processing of personal data across worldly nations or within particular regions provide the basis for discussion and limitation in this chapter. The former shall be referred to as 'universal system' which means frameworks of laws developed under the auspices of the United Nations (UN)[501]

---

[499] See, e.g., Mc Cullagh, p.1, note 372, supra; Roos, pp.405-406, note 2, supra; Loukidelis, D., 'Transborder Data Flows & Privacy-An Update on Work in Progress', Paper Presentation at the 7th Annual Privacy & Security Conference, Victoria, BC, February 10, 2006, pp.1-17, at pp.4-5, http://www.oipc.bc.ca/pdfs/Speeches/TransborderDataFlowsSpeech%2810Feb06%29.pdf last visited 9/12/2011.

[500] Bygrave notes that the 1978 French Act on data protection (*Loi no. 78-17 du 6. Janvier 1978 relative à l' informatique, aux fichiers et aux libertés*), applies to France's remaining overseas territories, such as Guadelope. Also, by virtue of s.2 of the Norway's 1985 Petroleum Act (*Lov om petroleumsvirksomhet 22. Mars 1985 nr.11*), the 1978 Norwegian Act on data protection (*Lov om personregistre mm. Av 9. Juni 1978 nr.48*) applies to offshore installations engaged in exploration, production and transport of petroleum products on the Norwegian continental shelf (and outside the Norwegian continental shelf if this is in accordance with international law or an agreement with a foreign state), see Bygrave, L.A., 'Determining Applicable Law pursuant to European Data Protection Legislation', Computer Law & Security Report, 2000, Vol.16, No. 4, pp.252-257, at p. 252.

[501] Some commentators like Hinz have questioned the universality of instruments made under the umbrella of UN more particularly the Universal Declaration of Human Rights (UDHR) 1948. Hinz's argument lies in the exclusion of participation of some members of the United Nations we see them today especially those which were still under colonial rule. Yet he acknowledges the great influence of the UDHR in legislating legal instruments and lying down

while the latter 'regional system' which means frameworks of laws developed under the auspices of regional organizations. Left unexamined in this chapter are instruments that regulate specific sectors as such instruments tend to follow the broad principles found in the general instruments.[502] However, general reference may be made to these instruments where necessary. Also, this chapter leaves unexamined the regional system of data privacy in Africa. Discussion of the latter is reserved for the next chapter (chapter four). It is also important not to confuse 'international law' in the sense referred here with the ability of national data privacy legislation to regulate transfer of personal data in other jurisdictions or to exercise some controlling hand on facilities located outside the national territory where such facilities are used to process personal data concerning individuals in that nation. This extra-territoriality of the national law is excluded from the purview of this chapter. Two reasons account for this exclusion. First, the principles enshrined in the national legislation are most invariably a transposition of the international law. Yet, the exercise of influence in the privacy field has not been unidirectional, flowing only from the international to the national plane.[503] National regulatory regimes have also inspired and shaped many international initiatives.[504] Second, as there are variations in the practices of national data privacy laws, it is difficult to transcend across those practices successfully. With these limitations, this chapter will make only general reference to national data privacy legislation where necessary to illustrate how broad principles under international law permeate the national domain.

---

the platform for the production of many conventions and treaties, Hinz, M.O., 'Human Rights between Universalism and Cultural Relativism? The Need for Anthropological Jurisprudence in the Globalising World', in A.Bösl and J.Diescho (eds)., Human Rights in Africa: Legal Perspectives on their Protection and Promotion, Macmillan Education Namibia, 2009, pp. 3-32, at p. 4. For more discussion about universalism-relativism see notes 43 & 44 supra.

[502] See e.g., General Assembly of the World Medical Association, 'Declaration of Geneva: A Physician Oath', Geneva, 1948; General Assembly of the World Medical Association, 'Declaration of Helsinki: Recommendations Guiding Medical Doctors in Biomedical Research Involving Human Subjects', Helsinki,1964; General Assembly of the World Medical Association, 'Declaration of Helsinki: Ethical Principles for Research Involving Human Subjects', Edinburgh, 2000; Council of Europe Convention for the Protection of human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine 1997; World Health Organisation Declaration on the Promotion of Patients' Rights in Europe 1994; Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(O.J.L 24, 30 January 1998, pp. 1-8); Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic telecommunications sector(O.J.L 201, 31 July 2002, pp. 37-47); Regulation (EC) 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies on the Community and on the free movement of such data(O.J.L 8, 12 January 2001, pp.1-22); Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (O.J.L 105, 13 April 2006, pp.54-63); ILO, Protection of Workers' Personal data, an ILO Code of Practice, Geneva, 1997; ILO, HIV/AIDS and the World of Work, an ILO Code of Practice, Geneva, 2001.

[503] Bygrave, L.A., 'International Agreements to Protect Personal Data' in G.Greenleaf and J.B. Rule(eds)., Global Privacy Protection: The First Generation, Edward Elgar Publishing Limited, Cheltenham,UK/Northampton, MA,USA, 2008, pp.15-49, at p. 17.

[504] Ibid.

3.2 Universal Systems

The universal systems of protection of privacy and personal data trace back their origins to the end of the Second World War (World War II) in 1945. With the exception of the United nations Guidelines for the Regulation of Computerized Personal Data Files 1990[505] (*UN Guidelines*), the rest of the instruments made under the umbrella of UN and discussed here took the form of human rights treaties. The latter were partly negotiated and made as a response to the traumas of fascist oppression prior to and during World War II.[506] As the fascist regimes depended largely on personal information under their control to target and attack humanity, it was important that such information be protected in these treaties.[507] Of significance for discussion here are the Universal Declaration of Human Rights 1948[508] (UDHR), International Covenant on Civil and Political Rights 1966[509] (ICCPR or Covenant) and *UN Guidelines*.

3.2.1 Universal Declaration of Human Rights 1948

This is the first international human right treaty to be adopted by the United Nations after the end of World War II. The UDHR was actually preceded by the *Nuremberg Trials*[510] which saw the

---

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

[506] Salmer, K.S., '*Elekronisk databehandling og rettssamfunnet*', in *Forhandling ved Det 30. Nordiske juristmøtet, Oslo 15-17. august 1984*(Oslo: Det norske styret for De nordiske jurstmøter, 1984), Part II, 41,44 cited in Bygrave, pp.108-109, note 24, supra.

[507] Hilbergy observes the following with respect to the persecution of Jews in Germany under the Nazi regime: 'The whole identification system, with its personal documents, specifically assigned names, and conspicuous tagging in public, was a powerful weapon in the hands of the police. First, the system was an auxiliary device that facilitated enforcement of residence and movement restrictions. Second, it was an independent control measure in that it enabled the police to pick up any Jew, anywhere, anytime. Third, and perhaps most important, identification had a paralyzing effect on its victims. The system induced the Jews to even more docile, more responsive to command than before. The wearer of the star was exposed; he thought that all eyes were fixed upon him. It was as though the whole population had become a police force, watching him and guarding his actions. No Jew, under those conditions, could resist, escape, or hide without first ridding himself of the conspicuous tag, the revealing middle name, the telltale ration card, passport, and identification papers. Yet the riddance of these burdens was dangerous, for the victim cold be recognised and denounced. Few Jews took chance. The vast majority wore the star and, wearing it, were lost.', Hilberg, R., The Destruction of the European Jew, Holmes & Meier Publishers, New York, pp.173-180.

[508] United Nations General Assembly, 'Universal Declaration of Human Rights', New York, United Nations, Resolution 217A (III), U.N.Doc A/810 at 71(1948).

[509] United Nations General Assembly, 'International Covenant on Civil and Political Rights 1966', New York, United Nations, Resolution 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999, U.N.T.S 171, entered into force on 23/03/1976.

[510] The Nuremberg Trials were a series of military tribunals, held by the victorious Allied forces of World War II, most notable for the prosecution of prominent members of the political, military, and economic leadership of the defeated Nazi Germany. The trials were held in the city of Nuremberg, Bavaria, Germany, in 1945–46, at the Palace of Justice. The first and best known of these trials was the Trial of the Major War Criminals before the International Military Tribunal (IMT), which tried 24 of the most important captured leaders of Nazi Germany, though several key architects of the war (such as Adolf Hitler, Heinrich Himmler, and Joseph Goebbels) had committed suicide before the trials began, see, http://en.wikipedia.org/wiki/Nuremberg_Trials last visited 6/12/2011.

prosecution of the perpetrators of the World War II most of them officials and soldiers under the Nazi regime. The *Universal Declaration* therefore constitutes a recognition of and pledge to basic human rights for the international community.[511] This pledge is reflected in the second and fifth recitals in the preamble of the UDHR:-

> 'Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind, and the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people; ....Whereas the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom.'

As its name suggests, the UDHR was not meant to be a legally binding instrument but rather a declaration in human rights. Structurally the *Universal Declaration* has a total number of eight recitals and thirty articles. Art 12 of the UDHR specifically declares privacy as a basic human right. This provision states, '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.' The language of Art 12 leaves it clear that only arbitrary interference with the right to privacy is prohibited as such not all infringements of privacy are necessarily prohibited.[512]

Besides Art 12, there are other provisions in the UDHR which more generally address privacy issues. This can be illustrated by Art 27(1) which clearly states, 'everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.' The phrase *'freely to participate'* in this provision reflects principles of consent which are quite often necessary in conducting health scientific researches.

Although Articles 12 and 27(1) of the UDHR afford protection of an individual's privacy they are not absolute. The two are subject to the general limiting clause of the UDHR. This limitation

---

[511] Canadian Institutes of Health Research (CIHR), 'Selected International Legal Norms on the Protection of Personal Information in Health Research' December, 2001, p. 6, ISBN 0-662-31428-IN, http://www.cihr-irsc.gc.ca/e/documents/protection_pi_e.pdf last visited 6/12/2011.
[512] Ibid.

is provided in Art 29 (2). The latter states, 'in the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.' The rationale behind these limitations is to attempt to balance the provisions on privacy with the other rights in the *Universal Declaration*. However actual limitations have to be provided in the national legislation taking into account issues of morality, public order and the general welfare in a democratic society.

It is pertinent to note that since the *Universal Declaration* is not legally binding, it provides for no mechanism to enforce it. Yet, the UDHR has been cited quite often in judgments of regional and national courts as the normative foundation of basic human rights.[513]

3.2.2 International Covenant on Civil and Political Rights 1966

The ICCPR is the second international human rights instrument to be made under the umbrella of the United Nations. Unlike the UDHR, ICCPR is a legally binding international instrument which was intended to elaborate on, and give legal effect and implementation to, the principles proclaimed in the *Universal Declaration*.[514] [515] The ICCPR is essentially a convention of civil and political rights. It has five recitals that reflect the spirit of the UDHR and fifty three articles.

Article 17 of the ICCPR protects the right to privacy. This provision states, '17(1) no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation.' It further underlines in 17(2), 'everyone has the right to the protection of the law against such interference or attacks.' Certainly because of consolidating the spirit of the *Universal Declaration*, Article 17 of the ICCPR adopts verbatim the language of Art 12 of the UDHR. Yet, in contrast to the latter, the Convenant does not contain the general

[513] See generally, O'Donnell, M.K., 'New Dirty War Judgements in Argentina: National Courts and Domestic Prosecutions of International Human Rights Violations', New York University Law Review, 2009, Vol.84, pp.333-374; see also Messele, R., 'Enforcement of Human Rights in Ethiopia', Research Subcontracted by Action Professionals' Association for the People(APA), 31st August 2002, Chapter 3, 3.1, Implementation of International Human Rights Instruments, http://www.apapeth.org/Docs/ENFORCEMENT%20OF%20HR.pdf last visited 6/12/2011.

[514] CIHR, p.8, note 511, supra.

[515] The general status with respect to the parties to the ICCPR is that up to 4/01/2010 there were 165 parties; see http://cil.nus.edu.sg/1966/1966-international-covenant-on-civil-and-political-rights-iccpr/ last visited 6/12/2011. However as of October 2011, this number has increased to 167 parties, 67 of which have signed and ratified the treaty while the rest by accession or succession. The rest five parties have only signed but have not yet ratified the treaty, http://en.wikipedia.org/wiki/International_Covenant_on_Civil_and_Political_Rights last visited 6/12/2011.

limiting clause similar to Art 29 of the UDHR. Moreover in contrast to the *Universal Declaration* which indirectly (Art 27(1)) upholds the spirit of the Nuremberg Code 1947,[516] Art 7 of the ICCPR expressly states:-

> 'No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected to medical or scientific experimentation.'

The implementation of the ICCPR is primarily left to the states parties.[517] At international level, the ICCPR provides for the establishment of the Human Rights Committee (HRC) as its oversight and complaints handling body.[518] The latter's jurisdiction is limited only to those states parties which have declared expressly to recognize the competency of the HRC.[519] Moreover, before a state party submits communications/complaints to the HRC, it has to ensure that all available domestic remedies have been invoked and exhausted in the matter.[520] Only after such attempts have failed a state party is allowed to submit the unresolved dispute to the HRC. If, after attempts by the HRC to resolve the dispute parties are still not satisfied then by prior consent they may appoint an *ad hoc* Conciliation Commission (CC) to resolve the matter.[521] In case parties do not still agree to the outcome of the conciliation made under the CC, they have to notify the HRC.[522] It is interesting to note that the views reached by the HRC in any of the complaints submitted under its jurisdiction are not binding under international law yet they carry a great deal of weight.[523] These views, along with the Committee's reports and general comments

---

[516] The first principle of the Nuremberg Code states, 'the voluntary consent of the human subject is absolutely essential. This means that the person involved should have legal capacity to give consent; should be so situated as to be able to exercise free power of choice, without the intervention of any element of force, fraud, deceit, duress, overreaching, or other ulterior form of constraint; and should have sufficient knowledge and comprehension of the elements of the subject matter involved as to be enable him to make an understanding and enlightened decision. This latter element requires that before the acceptance of an affirmative decision by the experimental subject there should be made known to him the nature, duration, and purpose of the experiment; the method and means by which it is to be conducted; all inconveniences and hazards reasonably to be expected; and the effects upon his health or person which may possibly come from his participation in the experiment. The duty and responsibility for ascertaining the quality of the consent rests upon each individual who initiates, directs, or engages in the experiment.'

[517] For detailed discussion on implementation of the ICCPR at national level see e.g., Frowein, J.A and Wolfrum, R(eds)., 'Domestic Implementation of the International Covenant on Civil and Political rights to its article 2 para 2', Max Plunk Yearbook of United Nations Law, 2001, Vol.5, pp.399-472.

[518] ICCPR, Art 28(1).

[519] Ibid, Art 41 (1).

[520] Ibid, Art 41 (1) (c).

[521] Ibid, Art 42(1), (a).

[522] Ibid, Art 42 (7), (c) & (d).

[523] Bygrave, p.248, note 288, supra.

to states parties under Art 40 (4) of the ICCPR, provide authoritative guidance on the scope of the Covenant's provisions.[524]

Also noteworthy is that the HRC is not a judicial body. As a result, the enforcement mechanism under the ICCPR remains relatively weak.[525] The International Court of Justice (ICJ) also lacks jurisdiction to deal with disputes arising from breaches of the ICCPR despite the fact that the ICCPR is a Convention made under the umbrella of the United Nations.[526] Judicial remedies with regards to matters provided in the ICCPR are only reserved for national courts.[527]

3.2.3 UN Guidelines for the Regulation of Computerized Personal Data Files 1990

In contrast to the UDHR and ICCPR, the *UN Guidelines* for the Regulation of Computerized Personal Data Files constitute the first efforts by the United Nations to develop concrete rules for protection of personal data.[528] The *UN Guidelines* were preceded by two regional instruments specifically made to regulate processing of personal data: the Organization for Economic Co-operation and Development (OECD), Guidelines on the Protection on Privacy and Transborder Flows of Personal Data 1980[529] (*OECD Guidelines*) and the Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981[530] (*CoE Convention 108/1981*). Perhaps because of this, the *UN Guidelines* are influenced by its predecessors more particularly the *OECD Guidelines*.

Two main objectives are at the core of the *UN Guidelines*: supply of broad minimum guarantees that should be incorporated in the national legislation of the member states[531] and encouraging governmental and non-governmental international organizations to apply the *Guidelines* in

---

524 Ibid.
525 Ibid.
526 Ibid; see also, Art 36 of the Statute of the International Court of Justice (ICJ), http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0 last visited 7/12/2011; Crook, J.R., 'The International Court of Justice and Human Rights', Northwestern University Journal of International Human Rights, 2004, Vol.1, pp.1-8, http://www.law.northwestern.edu/journals/JIHR/v1/2/Crook.pdf last visited 7/12/2011.
527 ICCPR, Art 2(3) (b).
528 Historically the *UN Guidelines* can be traced from the UN General Assembly Resolution 2450 of December 1968(Doc E/CN.4/1025) in which the UN Secretary-General was invited to examine the impact of technological developments on human rights, including consideration of individuals' right to privacy 'in the light of advances in recording and other techniques'. The resulting study by the Secretary-General led to the publication of a report in 1976 urging states to adopt privacy legislation covering computerised personal data systems in the public and private sectors, and listing minimum standards for such legislation, Bygrave, p.29, note 503, supra.
529 OECD Doc. C (80)58/FINAL, adopted on 23 September 1980.
530 ETS No. 108; opened for signature 28 January 1981; in force 1 October 1985.
531 *UN Guidelines*, PART A.

processing personal data.[532] To achieve the two objectives, the *UN Guidelines* lay down general principles concerning processing of personal data held in computerized files. These principles are provided in the form of non-legally binding guidelines. The responsibility of developing concrete detailed regulations for regulating personal data is left to states taking into account the principles spelt in the *UN Guidelines* as the minimum standard.

Structurally, the *UN Guidelines* contain ten provisions. There is neither a preamble preceding these provisions nor definition of terms in the *Guidelines*. Such omissions diminish considerably the *Guidelines'* practical utility.[533]

The scope and application of the principles provided in the *UN Guidelines* is primarily limited to the processing of personal data of natural persons in the public and private sector with respect to computerized files.[534] This limited scope can also be depicted from the long title of the *Guidelines*. However two exceptions may also apply. First, the principles contained in the *UN Guidelines* may be extended subject to appropriate adjustments to manual files.[535] Second, such principles may be exceptionally extended to files on juristic persons especially when they contain information on individuals.[536]

The *UN Guidelines* contain seven fair information processing principles of computerized personal files: lawfulness and fairness, accuracy, purpose specification, disclosure limitation, interested personal access, non-discrimination and security. These are usual principles of personal information processing found in most data privacy protection regulatory instruments (see 3.3). It is imperative to note that, there are interdependence in these principles. The implementation of one principle in practice requires the existence of the other. Thus although attempts to analyze these principles is made on each, one should not be mislead to think that each principle exists independently.

The first principle, *principle of lawfulness and fairness*, requires that information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.[537] This principle embodies

[532] Ibid, PART B.
[533] Bygrave, p.30, note 503, supra.
[534] *UN Guidelines*, Para. 10.
[535] Ibid.
[536] Ibid.
[537] Ibid, Para 1.

two criteria at a time, lawfulness and fairness. *Lawfulness* criterion is relatively self-explanatory.[538] It may simply mean that before any processing activity can take place the data controller must ensure that the intended processing is backed by an enabling instrument or consent from the data subject.[539] Unlike *lawfulness* criterion, *fairness* is more complicated to explain. Part and parcel of this complexity is the fact that *fairness* cannot be achieved in the abstract.[540] Also, general agreement on what is fair is inevitably subject to change.[541] Yet, despite these hurdles, fairness can generally mean the following: taking into account of data subjects' interests and reasonable expectations in the course of processing their personal information; unduly pressurizing data subjects to disclose information about them or accepting such information to be used for other particular purposes; transparency of the personal data processing activities; direct collection of personal data from the data subjects; abstaining from re-use of personal information collected for one purpose for other purposes than the one specified during collection; etc.[542]

The second principle is the *principle of accuracy*. According to this principle, persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular check on the accuracy and relevancy of the data recorded and to ensure that they are kept as complete as possible to avoid errors of omission and that they are kept up to date regularly or when information contained in a file is used as long as they are being processed.[543] Four criteria can be isolated from this principle: accuracy, relevancy, completeness and up-to-datedness. Information is considered accurate as long as it is correct and true in every detail and in any case it does not contain errors. This may entail a number of things. For example, to ensure that personal information is collected directly from data subjects; there are no omissions in such information in which case information becomes complete and most important such information is updated. As for relevancy of information, this criterion is linked to other principles. The purpose specification is one of such principles. At the same time both the requirements of relevancy and purpose specification operate to limit information collected to a minimum.[544]

---

[538] Bygrave, p.58, note 24, supra.
[539] See e.g Kalliopi Nikolaou v. Commission, Case T-259/03, European Court of First Instance, Luxembourg where the Commission was held in breach of Article 5 of Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data after disclosing leak information concerning Nikolaou which in the eyes of the Court constituted unauthorised transmission.
[540] Bygrave, note 538, supra.
[541] Ibid.
[542] Ibid, pp.58-59.
[543] *UN Guidelines*, Para 2.
[544] Bygrave argues that the *UN Guidelines* does not contain any express provision on the information minimality principle yet such requirement can be red into the more general criterion of the fairness as set out in Principle 1 of the *UN Guidelines*; Bygrave, p.60, note 24, supra.

The third principle is the *purpose specification*. This principle states that the purpose for which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that all personal data collected and recorded remain relevant and adequate to the purpose so specified; no disclosure of such information is made without consent of the person concerned and for purposes incompatible from those specified and the period for which such data is kept does not exceed achievement of the purpose specified.[545] The purpose specification principle is a cluster of many requirements. In the first place it requires the purpose for collection of personal data to be specified. This ensures to determine if such information is really relevant to achieve a specified purpose. Apart from that the purpose itself needs to be legitimate. The bulk of data protection instruments comprehend legitimacy *prima facie* in terms of procedural norms hanging on a criteria of lawfulness(e.g., that the purpose for which personal data are collected should be compatible with the ordinary, lawful ambit of the particular data controller's activities).[546] There is also a requirement of publicity or notification of data processing to the personal concerned. This requirement intends to ensure that data processing remains transparent to the persons concerned so that they can be able to ascertain if it is compatible with the purpose of its collection. Also it facilitates data subject's participation in the data processing activities.

The fourth principle is the *disclosure limitation*.[547] This principle is expressly embedded in the third principle above-i.e. *purpose specification*. It is also linked to the *interested-person access* which ensures that all disclosures of a data subject's personal information are brought into his or her attention with the purpose of seeking consent where applicable.

The fifth principle, *interested-person access*, provides that everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expenses, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entry and, when it is being communicated, to be informed of the addressees. This principle further states that provision should be made for a remedy, if need be with the supervisory authority. The costs of any rectification shall be borne by the person responsible for the file. Further that it is desirable the provisions of this principle should apply to everyone, irrespective of nationality or place of

[545] *UN Guidelines*, Para 3.
[546] Bygrave, pp.61-62, note 24, supra.
[547] *UN Guidelines*, Para 3(b).

residence.[548] 'Access' under this principle entails that a data subject possesses knowledge of processing of personal data about him or her. This includes knowing which information about him or her is held by the data controller and how such information is being used and for what purpose. The right of access is also being made meaningful if the data subject can cheaply in terms of both time and cost obtain in an intelligible form such information about him or her and the manner it is being used and processed by the data controller. Also part and parcel of the right of access is the ability of a data subject to demand rectification or erasure of such information which has been unlawfully obtained, irrelevant or contains inaccuracies. Moreover, the right of access entails that a data subject is specifically informed of the recipients of information about him or her. This is important because of controlling re-use of personal information for purposes other than those specified during collection. The interested- person access principle also requires that a person concerned is able to obtain appropriate remedy for correction or eraser at the expense of the data controller. Also important to note is the fact that the *UN Guidelines* require the right of access to apply to everyone irrespective of one's nationality or place of residence. This partly gives the *UN Guidelines* its universal character.

The sixth principle is *non-discrimination*. This principle requires that data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.[549] However exceptions for this rule are acceptable only within the framework of the provisions of the International Bill of Human Rights and other relevant instruments in the field of protection of human rights and prevention of discrimination.[550] Unlike other instruments (see 3.3) which deal with the same principle under *sensitivity*, the *UN Guidelines* deploy the term *non-discrimination*. Perhaps because of this, the latter does not address health information in its list while the former does. Also, the latter goes far to deal with discrimination on membership of an association in general while the former only stops at trade-union membership.

The seventh principle is about *security*. Accordingly appropriate measures are required to be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such unauthorized access, fraudulent misuse of data or contamination by computer viruses. Worthy note is that while security and privacy issues are not identical limitations on data

[548] Ibid, Para 4.
[549] Ibid, Para 5.
[550] Ibid, see also *UN Guidelines*, Para 6.

use and disclosure must be reinforced by security safeguards.[551] The measures envisaged under this principle include use of appropriate and up-to-date software, physical measures (e.g. looked doors and identification cards), trainings, pre-employment vetting and adoption of security codes.[552]

It is important to underline that the *UN Guidelines* does not specifically contain the *principle of minimality* as a standalone principle. This is in sharp contrast to other instruments (see 3.3) which deal with minimality as an independent principle. Nevertheless, the minimality requirement in processing personal data can still be read into other principles of the *Guidelines* more particularly *accuracy*, *fair processing* and *purpose specification*.

To ensure that the above principles are complied with, the *UN Guidelines* calls every country to designate a supervisory authority to offer supervision.[553] The *Guidelines* sets three attributes for such authorities: impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data and technical competence.[554] Also the supervisory authorities have to be empowered as part and parcel of such enforcement to inflict criminal sanctions as well as appropriate individual remedies in case of breaches of the above principles.[555] Aware of variations of domestic legal systems, the *Guidelines* directs that the designation of supervisory authorities must be fitting into such systems. Some jurisdictions have designated the Freedom of Information Act (FOIA) authorities as also discharging the function of data protection authorities.[556] Others have separated the two authorities to keep clear lines between them.[557] Yet, it must be admitted that even in such latter case there are intersection between the enforcement authorities hence cooperation between them is necessary.

There are also provisions as to regulation of transboder data flows in the *UN Guidelines*.[558] The *Guidelines* requires that when two countries in the context of transfer of personal data have

---

[551] Greenleaf, G *et al.*, 'Interpreting the Security Principle', Working Paper No.1, v.6 March 2007, pp.1-37, at 6, http://www.cyberlawcentre.org/ipp/wp/WP1%20Security.pdf last visited 10/12/2011.
[552] Ibid.
[553] *UN Guidelines*, Para 8.
[554] Ibid.
[555] Ibid.
[556] The UK Information Commissioner's Office (ICO) is a direct case to the point. The ICO supervises the Data Protection Act 1998; Freedom of Information Act 2000; Privacy and Electronic Communications (EC Directive) Regulations 2003 changed on 26 May 2011 and above all the Environmental Information Regulations 2004 which does not directly regulate processing of personal information.
[557] See e.g., the Norwegian Data Protection Inspectorate which only administers the Data Register Act 1978 now replaced by the Personal Data Act 2000.
[558] *UN Guidelines,* Para 9.

'comparable' safeguards in their laws regulating privacy information should be left to circulate freely in the two countries. Yet, if there are no reciprocal safeguards, the *Guidelines* require that such circulation may not be imposed unduly and only in so far the protection of privacy demands. Few questions may arise here. Who is to determine the comparability of safeguards? Certainly the supervisory authorities in the countries concerned. What are the criteria/parameters of comparison? What are the criteria that countries concerned should take into account not to impose unduly restrictions to the free flow of circulation of personal data? The *Guidelines* are silent on all these questions. Undoubtedly this silence may result into practical difficulties in their implementation.

An overview of the universal systems of privacy protection leads to the following conclusions. First, although the UDHR and ICCPR do not expressly spell principles of data protection they offer strong normative roots for the data protection laws in regional and national jurisdictions.[559] This normativity can well be noticed expressly or impliedly from the preambles and recitals of such regional and national legislation dealing with data protection. At national level, frequent reference to the UDHR and ICCPR in the preamble of the constitutions generally affirms the universal recognition and acceptance of these international documents within domestic legal systems. Since the right to privacy is incorporated in the Bill of Rights of such constitutions, it serves to domesticate the right to privacy found in the UDHR and ICCPR. Second, under the universal system only the *UN Guidelines* deals with data protection more specifically. Nonetheless such *Guidelines* have received relatively little attention as compared to the regional instruments on data protection specifically those in Europe (see 3.3). This is partly because the *Guidelines* are not legally binding and seem to have had little practical effect relative to the other instruments.[560] Indeed, the *Guidelines* tend to be overlooked in much data protection discourse, at least in Scandinavia.[561] The other reasons that may have significantly reduced the practical effect of the *UN Guidelines* is the fact that they came later in the 1990 after the *OECD Guidelines* 1980 and *CoE Convention 108/1981* had been in place and already influenced adoption of data protection legislation in many countries. Of course, this reason though may seem weak in the context of the adoption of Directive 95/46/EC in 1995 well after the *UN Guidelines* were already in place, it has to be understood that the scope of the former in terms of elaboration of the principles, binding

[559] See e.g., Bygrave, p.45, note 503, supra; Bygrave, p. 332, note 25, supra; Bygrave, p.180, note 27, supra; Kuner, p.309, note 264, supra.
[560] Bygrave, p. 33, note 24, supra; Bygrave, note 533, supra; Karanja, p.126, note 239, supra; Greenleaf, G., 'Asia-Pacific Developments in Information Privacy Law and Its Interpretation', New Zealand Privacy Issues Forum, 2006, pp.1-25, at pp5-6.
[561] Bygrave, p. 33, note 24, supra.

nature and enforcement institutions generally exceed far the latter. Moreover, the Directive 95/46/EC seems to incline more to the *OED Guidelines* and *CoE Convention 108/1981* than to the *UN Guidelines*. Third, the efforts to achieve a legally binding global data privacy treaty are far from reality. Calls for such an instrument are increasingly made, and work is underway to draft an appropriate set of international rules on point.[562] Yet, while there is clearly a need for a global legal approach in the field, there are, realistically, scant chances of say, a UN-sponsored convention being adopted in the short term.[563] This is partly because the differences in cultural, historical and legal approaches to data protection mean once one descends from the highest level of abstraction, there can be significant differences in details.[564]

3.3 Regional Systems

3.3.1 Europe

In relative terms data protection regimes in Europe are more developed than elsewhere in the world. These regimes have been produced under the initiatives of three main organizations: the Council of Europe,[565] OECD[566] and European Union.[567] Some instruments developed under the

[562] Bygrave, p.181, note 27, supra.
[563] Ibid; see also, Bygrave, p.333, note 25, supra; Bygrave, pp.48-49, note 503, supra; Kuner, pp.310-317, note 264, supra.
[564] Kuner, p.310, note 264, supra.
[565] The Council of Europe is an international organisation promoting co-operation between all countries of Europe in the areas of legal standards, human rights, democratic development, the rule of law and cultural co-operation. It was founded in 1949, has 47 member states(Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The former Yugoslav Republic of Mecedonia, Turkey, Ukraine, and United Kingdom) with some 800 million citizens, http://en.wikipedia.org/wiki/Council_of_Europe last visited 12/12/2011. The headquarters of the Council of Europe are in Strasbourg, France.
[566] As an international organisation, OECD was officially established on 30 September 1961, the date when it came into force. Currently the organisation has a total number of 34 member countries (Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, Netherland, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States). Historically, OECD grew out of the Organisation for European Economic Cooperation (OEEC) which was established in 1947 to run the US-financed Marshall Plan for reconstruction of a continent ravaged by WW II. By making individual governments recognise the interdependence of their economies, it paved the way for a new era of cooperation that was to change the face of Europe. Encouraged by its success and the prospect of carrying its work forward on a global stage, Canada and the US joined OEEC members in signing the new OECD Convention on 14 December 1960; http://www.oecd.org/document/25/0,3746,en_36734052_36761863_36952473_1_1_1_1,00.html,
last visited 12/12/2011. The headquarters of the OECD are in Château de la Muette, Paris (France).
[567]The European Union (EU) is an economic and political union of 27 member states which are located primarily in Europe. These countries include: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom. The EU traces its origins from the European Coal and Steel Community (ECSC) and the European Economic Community (EEC), formed by six

auspices of these organizations address privacy issues in the same manner as the UDHR and ICCPR. This is the case with the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950[568] (European Convention of Human Rights or ECHR), Charter of Fundamental Rights of the European Union 2000[569](the Charter or CFR) which was later repealed and replaced by the Charter of Fundamental Rights of the European Union 2010[570] and the Treaty Establishing a Constitution for Europe 2004.[571] In all these instruments, privacy protection issues are dealt remotely. Yet, their significance lies in the normative force they provide as the legal foundations for data privacy laws. However, there are three specific instruments which were developed under the initiatives of the Council of Europe, OECD and EU to regulate data protection issues. These include the OECD Guidelines on the Protection on Privacy and Transborder Flows of Personal Data 1980, Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (*CoE Convention 108/1981*) and Directive 95/46/EC. Up until recently, these regimes more than anything else have exerted enormous influence to non-European countries to adopt data privacy legislation in the European style. This influence has been elaborated in a number of influential scholarly works: 'The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108',[572] 'The EU Data Protection Directive: An Engine of a Global Regime',[573] 'The European Union Data Privacy Directive and International Relations',[574] and 'International Data Protection Conference: Convention 108 as a Global Privacy Standard?'[575]

---

countries in 1958. In the intervening years the EU has grown in size by the accession of new member states, and in power by the addition of policy areas to its remit. The Maastricht Treaty established the European Union under its current name in 1993. The latest amendment to the constitutional basis of the EU, the Treaty of Lisbon, came into force in 2009; http://en.wikipedia.org/wiki/European_Union last visited 12/12/2011. The headquarters of the European Union are in Brussels (Belgium).

568 CETS No.: 005, opening for signature on 4 November 1950, entry into force 3 September 1953; The Treaty is open for signature by the member States of the Council of Europe and for accession by the European Union.

569 O.J.C364, 18 December 2000, pp. 1-22.

570 O.J.C83, 30 March 2010, pp.389-403.

571 O.J.C310/01, 16 December 2004, pp.1-474.

572 Greenleaf, G., 'The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108', International Data Privacy Law, 2012, Vol.2, No.1; also cited as UNSW Law Research Paper No. 39, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299 last visited 12/12/2011.

573 Birnhack, M. D., 'The EU Data Protection Directive: An Engine of a Global Regime', Computer Law & Security Report, 2008, Vol.24, No.6, pp.508-520;

574 Salbu, S.R., 'The European Union Data Privacy Directive and International Relations', Vanderbilt Journal of Transnational Law, 2002, Vol.35, pp.655-595.

575 Polakiewicz, J., 'Convention 108 as a Global Privacy Standard?', Polakiewicz, J (2011) 'Convention 108 as a global privacy standard?', International Data Protection Conference, Budapest, 17 June 2011 (Head of Human Rights Development Department, Directorate General of Human Rights and Legal Affairs, Council of Europe, yet the paper is written in a personal capacity as such it does not necessarily reflect the official position of the Council of Europe), available from Council of Europe website Data Protection Home Page.

3.3.1.1 European Convention on Human Rights 1950

The Council of Europe adopted the ECHR just two years after the Universal Declaration of Human Rights 1948. The circumstances and context in which the ECHR arose were the same as those for the UDHR: healing the past experience of totalitarianism in Western Europe. Because of this, the ECHR reaffirms in its preamble (recitals 1, 2 and 3) the value entrenched in the UDHR.

The ECHR is the Council of Europe's treaty as such it was open for signature and ratification only to its members. All the 47 members of the Council of Europe have signed and ratified the instrument. They are therefore bound by it. Worthwhile to keep in mind is that while all EU member countries are also members of the Council of Europe, the European Union itself is not part of the Council of Europe hence not legally bound by the ECHR.

Structurally, the ECHR has a preamble of five recitals and fifty nine articles. Article 8 of the ECHR governs the protection of the right to privacy. This provision states:-

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests 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 contrast to Art 12 of the UDHR and Art 17 of the ICCPR which are formulated in terms of prohibition on 'interference with privacy', Art 8 of the ECHR is framed in terms of a right to 'respect for private life'.[576] Yet, sub-article 2 of Art 8 of the ECHR expressly provides for the prohibition on interference with 'respect for private life' except under specific conditions. There

[576] Bygrave, p. 249, note 288 supra; for detailed discussion of what is meant by 'private life' read Arostegui, H.T., ' Defining "Private Life" Under Article 8 of the European Convention on Human Rights by Referring to Reasonable Expectations of Privacy and Personal Choice', California Western International Law Journal, 2005, Vol.35, No.2, pp.153-202.

are also general derogations in Arts 17 and 18 of the ECHR. However these may not be applicable with respect to Art 8 of the ECHR since the latter has been provided with specific derogative conditions. It is arguable that the different ways in which Arts 12 and 17 of the UDHR and ICCPR respectively as well as Art 8 of the ECHR are formulated have little practical implication on the way they have been interpreted.[577]

Originally the ECHR established the European Commission of Human Rights and the European Court of Human Rights (ECtHR) as its enforcement bodies in event of breaches.[578] However in 1998 major reforms into the two bodies were carried out.[579] Such reforms saw the abolition of the European Commission of Human Rights. At the same time the reforms streamlined the ECtHR in terms of the composition of the Court, tenure of judges, jurisdiction of the Court, etc. All such reforms meant to increase the efficiency of the ECtHR in delivering justice. It is important to note that the enforcement body in the ECHR is stronger than those in the ICCPR.[580]

With regard to the protection of privacy under Art 8 of the ECHR, the ECtHR has so far delivered substantial case law. This case law has received extensive scholarly comments (see paragraph 2.2 of this thesis).[581] Suffice to say that the Strasbourg case law is far from sufficiently reading in the data protection principles in Art 8 of the ECHR, as a result while such potential to embrace core data protection principles exists, currently such case law falls short of the data protection law standards.

3.3.1.2 Charter of Fundamental Rights of the European Union 2000

The CFR is yet another effort by the European Union to consolidate respect of fundamental rights within the EU. The Charter sets out in a single text, for the first time in the European Union's history, the whole range of civil, political, economic and social rights of European

[577] See paragraph 2.2 of this thesis.
[578] ECHR, (original) Art.19.
[579] ECHR (new) Art.19 after adoption of Protocol No.11 (ETS No. 155) to the European Convention on Human Rights, entered into force 1 November 1998; see also Drzemczewski, A., 'The European Human Rights Convention: Protocol No. 11 Entry into Force and First Year of Application', Documentação e Direito Comparado, 1999, nos 79/80, pp.219-247.
[580] See the jurisdiction of the ECtHR in Art. 32 of the ECHR.
[581] For detailed discussion about the interpretation of Art. 8 of the ECHR read Bygrave, pp.247-284, note 288, supra; Karanja, Chapter 4(pp.86-124), note 239, supra; De Hert and Gutwirth, pp.3-44, note 274, supra; Taylor, N., 'State Surveillance and the Right to Privacy', Surveillance & Society, 2002, Vol.1, No.1, pp.66-85; Connelly, A.M., 'Problems of Interpretation of Article 8 of the European Convention on Human Rights', International and Comparative Law Quarterly, 1986, Vol.35, pp.567-593.

citizens and all persons residing in the EU.[582] Its legal status is binding to all 27 EU member states. Interestingly the CFR, unlike the ECHR, does not specifically make reference in its preamble to the UDHR and ICCPR. Instead it specifically reaffirms the ECHR, Social Charters adopted by the European Union and the Council of Europe and the case-law of the Court of Justice of the European Union (ECJ) and of the European Court of Human Rights.[583] Also important to note here is that the Charter is subject to interpretation by the courts of the Union (i.e. ECtHR and ECJ) and member states.[584] This is slightly different from the ECHR which is strictly speaking subject to the ECtHR although the ECJ takes also into account case law developed by the former in its interpretation of some other instruments, e.g. the Directive 95/46/EC.

The Charter has a preamble of six recitals and a total number of fifty four articles. Of particular relevance to the present thesis are Arts 7 and 8. The former i.e. Art 7 of the CFR is framed in terms of a right to 'respect for private life' similar to Art 8 of the ECHR. This provision states, 'everyone has the right to respect for his or her private and family life, home and communications.' Yet, two important differences can still be noticed. First, whereas Art 8 of the ECHR uses the term 'correspondence' Art 7 of the CFR uses 'communications' instead. The former seems to be narrower in scope by confining to such things as written correspondence (e.g. *Campbell v. United Kingdom*[585]) and telephone conversations (e.g. *Malone v. United Kingdom*[586]). On the other hand the term 'communications' in Art 7 of the CFR envisages wide range forms of communications including the modern communications technologies.[587] The second difference between Art 7 of the CFR and Art 8 of the ECHR is that the latter contains a limitation clause in its sub-Article 2 on the exercise of the right in Art 8(1) while the former does not. Yet, Art 7 of the CFR is not absolute. It is subject to the general limitations put in Art 52. It is interesting to note that in Art 52(3), the CFR clearly spells that in case it contains corresponding rights to those provided in the ECHR, then the meaning and scope of those rights in the CFR shall be the same as those in the ECHR. This implies that the limitations put in Art 8(2) of the ECHR also apply to Art 7 of the CFR because Art 7 of the CFR and 8(1) of the ECHR are materially the same.

---

582 Karanja, p.79, note 264, supra.
583 CFR, Recital 5.
584 Ibid.
585 (1993) 15 EHRR 137.
586 (1984) 7 EHRR 14.
587 House of Lords-European Union Committee, Eighth Report, 1999-2000 cited in Karanja, p.81, note 264, supra; see also, Dossow, R., 'The Interception of Communications and Unauthorised Access to Information stored on Computer Systems in the Light of the European Convention on Human Rights', pp.1-8, at p.3, http://www.europarl.europa.eu/meetdocs/committees/temp/20010322/dossowcoe.pdf last visited 14/12/2011.

The most important innovation of the CFR is its incorporation of Art 8 which specifically covers protection of personal data. This has never been the case with the previous human rights treaties. To be sure Art 8 of the CFR states:-

1. Everyone has the right to protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of 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.

3. Compliance with these rules shall be subject to control by an independent authority.

The above provision declares protection of personal data as a right in itself. This has the effect of lifting and giving data protection a human rights status.[588] Moreover, it lays down albeit in brief the data protection principles to wit: fair processing, purpose specification, lawful processing requiring authorization either by consent of the person concerned or law, rights of access and rectification. Although these principles do not expressly reflect entirely the eight data protection principles found in the Directive 95/46/EC and national legislation in EU member countries, other principles can still be read into such four principles. For example, the purpose specification can also embrace the limitation and data subject participation principles. Also the relevancy and non-disclosure principles can be read in the purpose specification. The CFR puts a requirement for introduction of independent regulatory authorities to control compliance with the data protection principles similar to most national data protection legislation. Apart from raising the status of data protection law to human rights status, the incorporation of Art 8 in the CFR which now exists side-by-side with Art 7 on protection of the right to privacy 'may also signal a separation of the right to privacy and data protection.'[589]

[588] Karanja, p.81, note 264, supra.
[589] Ibid.

3.3.1.3 Treaty Establishing a Constitution for Europe 2004

Also known as the European Constitution or Constitutional Treaty, the Treaty Establishing a Constitution for Europe 2004 (TCE) which stands to date unratified presents a big blow to the elevation of the status of human rights and protection of personal data to a constitutional level in the European Union. Signed in Rome (29 October 2004) by the heads of states and governments of the EU member states, the European Constitution aimed at consolidating into a single text with some adjustments various pre-existing treaties regulating different matters in Europe with a view of fostering integration.[590] Summarizing this broad aim Piris posits:-

> 'The Constitutional Treaty aimed at "One Treaty, One Legal Personality and One Pillar." It repealed the two main existing Treaties-that is the EC and EU Treaties, as well as the previous Treaties and Protocols. The substance of all these Treaties was to be merged into a single "Constitutional Treaty". Only the Euratom Treaty would remain separate.'[591]

Worthwhile to note, the ratification of the Constitutional Treaty crumbled following the rejection of the text by two historic referendums in May 2005 and June 2005 in France and the Netherlands respectively. Despite that, it is still important to review the Constitutional Treaty for two reasons. First, is to analyze the would be implications of the Treaty on protection of human rights and personal data in the Union had it been successfully ratified. Second and equally important is to understand the implications of the failure of such ratification process on the same aspects. This second reason is further reinforced by the adoption of the Lisbon Treaty 2007[592] in the aftermath of the rejection of the Constitutional Treaty. In other words, to what extent the Lisbon Treaty 2007 retained the provisions of the Constitutional Treaty in as far as human rights and data protection is concerned? What are the effects of such retention? These questions need to be explored not just for academic purpose but to underscore if the Lisbon Treaty has any meaningful implications to the protection of human rights and data protection in

---

[590] For detailed discussion on the origin, negotiations and adoption of the Constitutional Treaty see e.g., Toops, E.E., 'Why is there No EU Constitution? An Analysis of Institutional Constitution-Making in the European Union', B.A Thesis, University of Pennsylvania, 2010; Phinnemore, D., 'The Treaty Establishing a Constitution for Europe: An Overview', The Royal Institute of International Affairs, 2004, pp.1-23; Archick, K., 'The European Union's Constitution', Congressional Research Service(CRS) Report for Congress, 2005, pp.1-6; Qvortrup, M., 'The Three Referendums on the European Constitutional Treaty in 2005', The Political Quarterly, 2006, Vol.77, No.1, pp.86-97; Zoller, E., 'The Treaty Establishing a Constitution for Europe and the Democratic Legitimacy of the European Union', Indiana Journal of Global Legal Studies, 2005, Vol.12, No.2, pp.390-408.

[591] Piris, J.C., The Lisbon Treaty: A Legal and Political Analysis, Cambridge University Press, UK, 2010, p.21.

[592] O.J.C 306, 17 December 2007, pp.1-271; entered into force on 1 December 2009.

the European Union. Yet before venturing into such discussion the structure of the Treaty needs a brief examination.

The Constitutional Treaty is the longest Treaty in Europe. Structurally, it has a preamble of seven recitals, four hundred and forty eight Articles and thirty six Protocols. The substantive parts of the Treaty are divided into four parts comprising many Titles in each. Of direct relevance for discussion here are some of the provisions in Title II and IV of Part I of the Treaty. Art I-9(1) under Title II gives the Charter of Fundamental Rights (CFR) the status of binding primary Union law. Worthwhile to keep in mind is that when the CFR was adopted in 2000 it was not legally binding to the Union. The Charter itself is wholly incorporated in the Constitutional Treaty (Arts II-61 to II-114). Apart from recognizing the Charter of Fundamental Rights, the Constitutional Treaty goes further to require the European Union in Art I-9(2) to accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). As pointed out the ECHR was not binding on the European Union as such but on its member countries. In this way, the Constitutional Treaty had the effect of upgrading both the CFR and ECHR to the binding Union law at a constitutional level.[593]

In the context of the protection of privacy and personal data, the upgrading of both the CFR and ECHR to the Union law would have had a wide range of implications. First, the provision of Art 8 of the ECHR and the case law developed thereon by the European Court of Human Rights in Strasbourg would have found their way in the European Union. This equally means that the European Court of Justice (ECJ), the Court for the European Union, which formerly did not pay sufficient attention to the case law of the ECtHR would now be compelled to do so by the Treaty.[594] Second, the entirely integration of the CFR into the Treaty would have given the CFR a binding force meaning that the provision of Art 7 on protection of privacy which is quite similar to Art 8 of the ECHR and which corresponds to Art II-67 of the Constitutional Treaty would have settled the old conflict between the European Parliament, some EU member states and the ECJ on the accession of the EU to the ECHR.[595] At the same time Art 8 of the CFR on protection of personal data which corresponds to Art II-68 of the Constitutional Treaty would have also acquired a binding force. Moreover, it would have raised the protection of personal

[593] Morjn, J., 'Balancing Fundamental Rights and Common Market Freedoms in Union Law: Schmidberger and Omega in the Light of the European Constitution', European Law Journal, 2006, Vol.12, No.1, pp.15-40, at p.17.
[594] See the hand-offs approach of the ECJ with regard to the interpretation of ECHR in Morjn, p.19, note 593, supra.
[595] Karanja, p.82, note 239, supra. Also see Art I-9(2) of the Constitutional Treaty which states, 'The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession to the Convention shall not affect the Union's competences as defined in the Constitution'.

data to the constitutional status taking into account that currently the specific right to the protection of personal data as a right under the national constitutions is found in only a handful EU member states.[596] The Constitutional Treaty would have also transcended the Pillar systems in as far as data protection issues are addressed in the Union laws. It has to be noted that in EU data protection covers mainly matters falling under the First Pillar as internal market related issue. The Second and Third Pillars relating to the areas of police and judicial cooperation on the one hand and common foreign and security policy on the other respectively are generally excluded from the application of Directive 95/46/EC (see 3.3.1.6). The Constitutional Treaty would have therefore merged the First and Third Pillars though of course it is still unclear how rigorously the European Court of Justice would be willing to examine issues previously treated as Third Pillar issues.[597] Moreover, the Treaty would have also extended its application to issues in the Second Pillar.[598]

Another reference to the protection of personal data in the Constitutional Treaty is found in Title IV of Part I in Art I-51. This provision states:-

1. Everyone has the right to the protection of personal data concerning him or her.

2. European laws or framework laws shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of the Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

Worthwhile to keep in mind is the fact that the above provision seems to be influenced by an already existing regulation in the European Union: the Regulation (EC) No.45/2001 on protection of individuals with regard to the processing of personal data by Community

[596] Cannataci, J.A and Bonnici, J.P.M., 'Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty', Information & Communications Technology Law, 2005, Vol.14, No.1, pp.5-15, at p. 11.
[597] Ibid, p.12.
[598] TCE, Part I, Title V, Arts I-40 & I-41; see also Hijmans, H and Scirocco, A., 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?', Common Market Law Review, 2009, Vol.46, pp.1485-1525, at p.1498; see also Di Fabio, D., 'The European Constitutional Treaty: An Analysis', German Law Journal, 2004, Vol.5, No.8, pp.945-956, at p.945 for further discussion about the abolition of the pillar systems in EU laws by the Constitutional Treaty.

institutions and bodies and on the free movement of such data. The reinstatement of this Regulation in the Constitutional Treaty had similar effect of elevating it to a constitutional level.

As pointed out, the Constitutional Treaty did not take effect because of the French and Dutch rejection in their referendums. After this failure a 'renegotiation' of the Constitutional Treaty manifested in the process initially under the German six-month presidency of the European Union that culminated in the adoption of the Lisbon Treaty in 2007, also known as the Reform Treaty and Treaty on European Union(TEU or simply EU Treaty). The latter Treaty was signed on 27 December 2007 and came into force on 1 December 2009 after the process of ratification was fully completed by the member states. Majority analysts have assessed that over 90% of the substance of the Constitutional Treaty had been preserved in the Lisbon Treaty.[599] Alexander Stubb, the then Finnish foreign minister and expert who represented the Finnish Government in the intergovernmental conferences of the European Parliament's Committee on Constitutional Affairs leading to the Lisbon Treaty raised this per cent to 99.[600]

With regard to issues of protection of human rights and personal data the Lisbon Treaty brought about two important elements. First, the Treaty left out the Charter of Fundamental Rights of the European Union (CFR) which was previously inserted in the Constitutional Treaty. Instead, it only made reference to CFR while at the same time making it legally binding instrument.[601] Some commentators like Bonde appears to argue that there is no real difference in publishing the Charter as an independent Part II of the Constitution and leaving it in a Treaty Article, as is done in the Lisbon Treaty.[602] The Charter's provisions would be made legally binding in exactly the same way as if they were explicitly set out in the Treaty itself.[603] Arguably, this view misses one point: in the Constitutional Treaty the Charter of Fundamental Rights would have had a constitutional status over and above being made legally binding. In support of this view Somek argues:-

> 'As regards fundamental rights, the muddle created by Article I-9 Constitutional Treaty remains unresolved (Article 6 EU Treaty). In fact, it is

[599] Archick, K and Mix, D.E., 'The European Union's Reform Process: The Lisbon treaty', Congressional Research Service (CRS) Report for Congress, 2009, pp.1-9, at p.3.
[600] Bonde, J.P., From EU Constitution to Lisbon Treaty, Foundation for EU Democracy and the EU Democrats in cooperation with Group for Independence and Democracy in the European Union, p.26, http://www.eudemocrats.org/eud/uploads/downloads/e-Lissabon_til_nettet.pdf last visited 20/12/2011.
[601] Lisbon Treaty, Art. 6(1).
[602] Bonde, pp.60-61, note 600, supra.
[603] Ibid.

exacerbated by the fact that the Charter now remains outside the ambit of the document.'[604]

The second element brought by the Lisbon Treaty is the duality of systems of interpretation of human rights in Europe. Art 6(2) requires EU member countries to accede to the European Convention of Human Rights and Fundamental Freedoms (ECHR) just like it was under the Constitutional Treaty.[605] Moreover, it makes fundamental rights emanating from the ECHR and constitutional traditions of member states the general principles under the Union law.[606] Under the Lisbon Treaty the European Union got for the first time a code of common fundamental rights of its own just as with other states.[607] In this case, the supreme interpreter of fundamental rights will now be the European Court of Justice, just as it is the case with supreme courts in the EU member states.[608] Now if there is conflict between European human rights standards as laid down in the ECHR and the interpretation by the ECJ, then the EU will prevail.[609] As the Lisbon Treaty ousts the jurisdiction of national courts of EU member states by requiring them to lodge complaints against other countries or itself through the ECJ, there is therefore risks of having two kinds of human rights in Europe: those that apply to all the European countries that have acceded to the ECHR and to its Court in Strasbourg; and those that only apply in the European Union and its own Court in Luxembourg.[610] This would have not been the case had the Constitutional Treaty been successfully ratified. While the same effect would still be present, in the Constitutional Treaty, that would have been somewhat mitigated given the great force the Constitution would exert towards the national courts as well as across Europe.

3.3.1.4 OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data 1980

The *OECD Guidelines* comprises the first clearest international efforts towards regulation of personal data. There were three main catalysts that led to the adoption of these *Guidelines* on 23 September 1980. Michael Kirby, the Chairman of the OECD Expert Group that worked on the formulation of the *Guidelines*, explains these catalysts in his most recent article, 'The History,

[604] Somek, A., 'Postconstitutional Treaty', German Law Journal, 2007, Vol.8, No. 12, pp.1121-1132, at p.1124.
[605] Constitutional Treaty, Part I, Title II, Art I-9(2).
[606] See Lisbon Treaty, Art 6 (3) and Constitutional Treaty, Part I, Title II, Art I-9(3).
[607] Bonde, p.34, note 600, supra.
[608] Ibid.
[609] Ibid.
[610] Ibid, p.35.

Achievement and Future of the 1980 *OECD Guidelines* on Privacy'[611] to comprise the following: the international character of transborder data flows (TBDF) which necessitated for an intercontinental solution; the rise and fast changing technology of informatics with its capacity to expand and expedite the analysis of personal data and to create connections not otherwise perceived was recognized as presenting new problems for privacy as that notion was to be understood in its wider, modern sense; and the changing nature of law in the latter part of the twentieth century as a discipline of nation states with territorial application to international law and policy. All these factors operated in interdependence. For example, the TBDF was actually fueled by the development of technology. Faced with these challenges the OECD resorted into developing the *OECD Guidelines*.

a) Philosophical Basis

In order to clearly understand the nature, character and scope of the *OECD Guidelines* and their fair information principles, it is imperative to underscore the philosophical basis underpinning the *Guidelines*. As pointed earlier (see footnote 566) the OECD is an international organization which grew out of efforts of economic reconstruction that was heavily destructed by the World War II. Its central tenets therefore lay in recognition of economic interdependence. Although OECD draws its members within and outside of Europe, it is worth to point out that majority of OECD member countries are European. Outside of Europe there are other influential countries such as the United States, Canada, Japan, Australia, New Zealand and Korea.[612] Seen from this context, the OECD body is a mix of different countries brought together under economic co-operation. Because of this, the philosophical basis of the *OECD Guidelines* is rooted in economic orientation rather than human rights sentiments. Jon Bing, the influential Norwegian professor at Norwegian Research Centre for Computers and Law (NRCCL), pounds this point by positing that the OECD, as its name applies, is principally interested in trade and the economic aspects of cooperation between member countries.[613] The *OECD Guidelines* therefore focuses on data protection and its impact on international trade and economic cooperation.[614] Similar views are lauded by Roger Clarke, one of the most critics of the *OECD Guidelines*, who argues that the Organization for Economic Cooperation and Development(OECD), formed in 1961, is a 'club

[611] Kirby, M., 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy', International Privacy Law, 2011, Vol.1, No.1, pp.6-14 at pp. 6-8.
[612] For a complete list of the current OECD member countries see, note 566, supra.
[613] Bing, J., 'The Council of Europe Convention and the OECD Guidelines on Data Protection', Michigan Yearbook of International Legal Studies, 1984, Vol.5, pp.271-304 at p. 272.
[614] Ibid.

of like-minded countries that provides governments a setting in which to discuss, develop and perfect economic and social policy'.[615] In practice, its focus is much more on economic rather than on social matters, with just one of its 15 Committees and associated Directorates addressing all of Education, Employment, Labour and Social Affairs.[616] The philosophical perspectives of the OECD are also well captured by Kirby himself where he stresses that ordinarily the OECD is not concerned with human rights protection.[617] In different occasions Kirby has repeatedly held:-

> 'It was the fear that local regulation, ostensibly for privacy protection, would, in truth, be enacted for purposes of economic protectionism, that led to the initiative of the OECD to establish the expert group which developed its Privacy Guidelines. The spectre was presented that the economically beneficial flow of data across national boundaries might be impeded unnecessarily and regulated inefficiently producing a cacophony of laws which did little to advance human rights but much to interfere in the free flow of information and ideas.'[618]

It is interesting to note that in his book *Data Protection Law: Approaching Its Rationale, Logic and Limits*[619] Bygrave took a different view from that of Kirby who wrote its foreword. Based on the empirical study conducted by Ellger, he (Bygrave) argues that very little solid evidence has been provided to back up the allegations of economic protectionism.[620] Bygrave illustrates concerns behind adoption of national data protection legislation in Norway, Germany, Austria, Sweden, France and the UK as not solely lying in the protectionism theory. He, however, admits that protectionism theory can less easily be refuted with respect to the adoption of the Directive 95/46/EC. Much evidence exists to indicate that the EC Commission, together with the Council of Ministers, first took up the issue of data protection in the 1970s largely out of concern for

---

615 Clarke, R., 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century', Xamax Consultancy Pty Ltd, 2000, pp.1-38, at p.8, http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html last visited 22/12/2011.
616 Ibid.
617 Kirby, p.7, note 611, supra; see also, Kirby, M., 'Privacy Protection-A New Beginning?', Prometheus, 2000, Vol.18, No.2, pp.125-132, at p.125.
618 Kirby, M., 'Legal Aspects of Transborder Data Flows', International Computer Law Adviser, 1991, Vol.5, No.5, pp.4-11, at pp. 5-6; see also Kirby, M., 'Legal Aspects of Transborder Data Flows', Global Telecommunications Congress and Exhibition, Vancuvouver BC Canada, 25 October 1990, Inter Comm, 90, pp.1-23, at p.7, http://www.michaelkirby.com.au/images/stories/speeches/1990s/vol22/839-Intercomm_90,_Vancouver_-_Legal_Aspects_of_Transborder_Data_Flow.pdf last visited 22/12/2011.
619 Bygrave, pp. xi-xiv, note 24, supra.
620 Ibid, p.114.

fostering development of the internal market and European IT-industry.[621] In rejecting the influence of protectionism arguments (aired mainly from the North American quarters) with regard to the emergence of the *OECD Guidelines*, Bygrave has recently argued that the *Guidelines* urge member states in paras 2 and 6 to take legal measures for 'the protection of privacy and individual liberties.'[622] Yet, the language of 'protection of privacy and individual liberties' is merely a disguise of the economic motivations which seem to feature prominently in the *Guidelines* and in the title of the *OECD Guidelines* themselves: 'Protection of Privacy and Transborder Flows of Personal Data'. Moreover, the incorporation of the language of 'the protection of privacy and individual liberties' may reflect the tensions that occupied the negotiation table by the Expert Group and an attempt to reconcile them in favour of the European member states in the OECD whose memories of the World War II were still fresh. Kirby's narration of these memories deserves to be recorded here:-

> 'Before and during the work of the expert group, numerous seminars and conferences were held in Paris and elsewhere concerned with aspects of the problems that led to the creation of the group. One of these was a large conference in Paris attended by the then President of the French Republic (Mr. Valéry Girscard d'Estaing). In the course of that conference, to which I contributed, the powerful feeling that lay behind the European response to the dangers to privacy was brought home to me in a vivid way. During an interval for public participation, an audience member leapt to his feet. I knew that his contribution would be unusual. His appearance was arresting. He had a long beard and his eyes gleamed as he spoke.'[623]

The unnamed audience whose contribution was appealing to the strong memories of the World War II posited:-

> 'Why, Mr. President, did so many refugees in France survive during the War? Why did so few resistance fighters and Jews survive in The Netherlands?, he said. 'It happened because, in the 1930s, The Netherlands government, with typical efficiency, had devised an identity card with a metal bar installed through the photograph. In France, we had an ordinary photograph, pasted on

[621] Ibid, p.115.
[622] Bygrave, p.27, note 503, supra.
[623] Kirby, p.9, note 611, supra.

> cardboard. It was easily imitated. Upon that difference hung the lives of thousands of good people. In France, they survived. In The Netherlands they perished. Efficacy is not everything. A free society defends other values. Personal control over data is one such value.'[624]

The above statements clearly indicate that the *OECD Guidelines* are not grounded in human rights. It is therefore unsurprising that the *Guidelines* do not make sound reference to the major international human rights treaties such as the UDHR and ICCPR as its normative roots.

b) Structure and Nature

Traditionally what are referred to as the *OECD Guidelines* are mere Annex to the OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data adopted on 23 September 1980. This Recommendation categorically restates in its preamble the foundations of the OECD by stating:-

> 'The Council, Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960… (stating)
>
> ***Article 1***
>
> The aims of the Organisation for Economic Co-operation and Development (hereinafter called the 'Organisation') shall be to promote policies designed: (c) to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.
>
> ***Article 3***
>
> With a view to achieving the aims set out in Article 1 and to fulfilling the undertakings contained in Article 2, the Members agree that they will: (a) keep each other informed and furnish the Organisation with the information necessary for the accomplishment of its tasks;

[624] Ibid.

Article 5

In order to achieve its aims, the Organisation may: (b) make recommendations to Members.'

To this Recommendation, there are the *OECD Guidelines*. These *Guidelines* are divided into five Parts. Part one deals with general definitions as used in the *Guidelines* as well as their scope. In total part one has six paragraphs (1-6). Part two which is central to the *Guidelines* deals with the basic principles of national application. The fair information practice principles are comprised in this part which has eight paragraphs (7-14) corresponding to the eight data protection principles. Part three addresses basic principles of international application. It is this part which contains regulations on transborder data flows (TBDF). Part three has four paragraphs (15-18). Part four deals with national implementation in just a single paragraph (19). Part five has three paragraphs (20-22). This part deals with matters of international co-operation.

Apart from the *Guidelines* which are the integral part to the Council Recommendation, there is also the Explanatory Memorandum (*OECD Guidelines* Explanatory Memorandum or EM). The major aim of the Memorandum is to provide explanation and elaboration to the contents of the *Guidelines* which are broadly formulated to reflect the debate and legislative work which had been going on for several years.[625] As the *Guidelilines*, The Explanatory Memorandum was also developed by the Expert Group. In total, the Explanatory Memorandum has two main parts with 77 numbered paragraphs. Part I deals with the general background leading to the adoption of the *OECD Guidelines*. Part II is subdivided into sub-parts A and B. The former addresses the purpose and scope of the *Guidelines* while the latter deals with detailed comments. It is important to mention that the Explanatory Memorandum serves only as a tool of interpretation for the *OECD Guidelines*. It does not in itself vary the meaning of the *Guidelines*.[626] In any case, it is subordinate to the *Guidelines*.[627]

The *OECD Guidelines*, as its name suggests, are not legally binding upon OECD member states. This non-binding nature of the *Guidelines* is not accidental. They were indented to be so. Kirby puts forward three main reasons why the OECD decided not to adopt a legally binding treaty or convention. First, by 1978, it was already obvious that the largest player in the processing of

[625] OECD, OECD Guidelines on the Protection of Personal Data and Transborder Flows of Personal Data, OECD Publication Service, Paris, 2001, p.21.
[626] Ibid.
[627] Ibid.

automated data (including for airlines, hotels, business, insurance, and banking information) was the United States of America.[628] Securing the agreement of that major economic player to a binding treaty presented two apparently inseparable obstacles: the need, in the ratification of any such treaty, for the concurrence of the United States Senate, traditionally suspicious of such engagements and the strong affirmation of free flows of information expressed in the First Amendment of the United States Constitution.[629] Undoubtedly these difficulties became real in 1990s when the United States with all its muscles resisted the pressure of the European Directive 95/46/EC which requires third countries to develop legislation which provides 'adequate' level of protection of personal data to the EU law. This resistance resulted into negotiation of the weak Safe Harbor Agreement (see 3.3.2). Second, for the European member countries, impairment of personal privacy was not a theoretical danger.[630] It was one deeply remembered from the misuse of personal data by security and military personnel during the Second World War, still a comparatively recent memory in 1978.[631] Third, there was suspicion by several non-European countries that the European treaty approach to protecting privacy was heavy-handed with bureaucracy; potentially expensive to implement; insufficiently sensitive to the values of TBDF; and (even possibly) motivated by economic protectionism so as to strengthen the European technology of informatics behind legally established data protection walls.[632] At the same time, Europeans were suspicious that the non-European member states would insist on a 'toothless tiger'.[633] They would give the appearance of agreement; but without any real or practical effectiveness.[634] In the above context of a wide range of conflicting interests the Expert Group's solution resided in the adoption of the non-legally binding *Guidelines*.

c) Objectives and Scope

The objectives for adoption of the *OECD Guidelines* can be read in the preamble of the Recommendation of the Council, where the *Guidelines* are annexed and from part two of the *Guidelines* themselves. The Explanatory Memorandum 25 summarizes these objectives into four:-

First, is to achieve acceptance by member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data. Second, is to reduce differences

[628] Kirby, p.8, note 611, supra.
[629] Ibid.
[630] Ibid.
[631] Ibid.
[632] Ibid, pp.8-9.
[633] Ibid.
[634] Ibid.

between relevant domestic rules and practices of member countries to a minimum. The third objective of the *Guidelines* is to ensure that in protecting personal data consideration is given to the interests of other member countries and the need to avoid undue influence with the flows of personal data between member countries. Fourth, is to eliminate as far as possible, reasons which might induce member countries to restrict transorder flows of data because of the possible risks associated with such flows.

The *OECD Guidelines* have a broad ambit. They apply to the private and public sectors including the police and national security agencies.[635] However, in the later case, the *Guidelines* explicitly provide exceptions in Para 4 that may be made based on national sovereignty, national security and public policy. Such exceptions are subject to two conditions: they must be as few as possible and be made known to the public.[636] In terms of content, the *Guidelines* extend their reach to both manual and electronic processing of personal data.[637] Explanatory Memorandum 37 clearly affirms this wide scope of the application of the *Guidelines* by providing that the principles for the processing of privacy and individual liberties expressed in the *Guidelines* are valid for the processing of data in general, irrespective of the particular technology employed. The *Guidelines* can therefore be expressed in the technological neutral terms.[638] [639] Yet, Para 3(c) of the *Guidelines* still permit member states to restrict the application of the *OECD Guidelines* only to automatic processing of personal data. However, the latter must be taken as exception and not the general rule in itself.[640]

The scope of the *OECD Guidelines* is also delimited by terminologies employed by them. Seen that way, the *OECD Guidelines* are based wholly on the basic concept of *personal data* as opposed to many national data privacy legislation including the Council of Europe Convention 108/1981 which are based on the concept of *personal data system.*[641] Yet, the *Guidelines* also presume some

---

635 *OECD Guidelines*, Para 2; see also Explanatory Memorandum 44.
636 *OECD Guidelines*, Para 4(a) & (b).
637 Ibid, Para 2.
638 Kirby, p.10, note 611, supra; see also Explanatory Memorandum 38.
639 Roger Clarke (p. 12 note 615, supra) suggests that the *Guidelines* carry within them self-contradictions when they purport to apply generally without restrictions of technology or otherwise (Explanatory Memorandum 37) while putting such restrictions in Para 3 (b) of the *OECD Guidelines*. Clarke has in fact relied on Explanatory Memorandum 45 which excludes 'trivial' cases of collection of personal data. Frankly, Clarke had incompletely absorbed the import of Para 3(b) of the *Guidelines*. Explanatory Memorandum 45 stresses that such exclusion should not mean that Paragraph 3 of the *Guidelines* is to be regarded as a vehicle for demolishing the standards set up by the *Guidelines*. But, generally speaking, the *Guidelines* do not presuppose their uniform implementation by member countries with specific details.
640 For detailed reasons why the Expert Group avoided restricting the scope of the *OECD Guidelines* see Explanatory Memorandum 35.
641 Bing, p.273, note 613, supra; see also Roos (LL.D Thesis), p.158, note 2, supra.

restructuring of the data; they therefore do not apply to single data elements.[642] They define *personal data* as any information relating to an identified or identifiable individual (data subject).[643] The Explanatory Memorandum elaborates further that *personal data* and *data subject* serve to underscore that the *Guidelines* are concerned with physical (natural) persons.[644] They allude to their extension to legal (juristic) persons more obliquely.[645] Paragraph 3 suggests that the *Guidelines* should be applied flexibly.[646] Although this paragraph contains no explicit reference to legal persons, the Explanatory Memorandum states, 'protection may be afforded to data relating to groups and similar entities whereas such protection is completely nonexistent in another country.'[647] An equally important terminology to understand apart from *personal data* is *data controller*. The latter is defined in Para 1(a) of the *OECD Guidelines* as a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that third party or by agent on its behalf. According to the Explanatory Memorandum, the definition of a *data controller* attaches responsibility for activities concerned with the processing of personal data. The *data controller* may be legal or natural person, public authority, agency or any other body but excludes (a) licensing authorities and similar bodies which exist in some member countries and which authorise the processing of data but are not entitled to decide(in the proper sense of the word) what activities should be carried out and for what purposes; (b) data processing service bureaux which carry out data processing on behalf of others; (c) telecommunications authorities and similar bodies which act as mere conduits; and (d) 'dependent uses' who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc.[648] The final terminology which has implications on the scope of the *OECD Guidelines* is *transborder flows of personal data*. This term means movements of personal data across national border.[649] It restricts the application of certain provisions of the *Guidelines* to international data flows and consequently omits the data flow problems particular to federal level.[650]

One point has to be made in connection with definitions of terminologies in the *Guidelines*. The list of such terminologies is kept short. The *OECD Guidelines* define only three terminologies. Important terms such as *data processing* remain undefined as such reference to *data processing* has

[642] Ibid; see also Explanatory Memorandum 38.
[643] *OECD Guidelines*, Para 1(b).
[644] Explanatory Memorandum 41.
[645] Bing, p.274, note 613, supra.
[646] Ibid.
[647] Ibid; see also Explanatory Memorandum 45.
[648] Explanatory Memorandum 40.
[649] *OECD Guidelines*, Para 1(c).
[650] Explanatory Memorandum 42.

been frequently associated to data collection. This may have the effect of undermining the implementation of the *Guidelines* in practice.

d) Data Protection Principles

The *OECD Guidelines* contain eight data protection principles. These need to be treated as a whole because there is some degree of duplication and the distinctions between different activities and stages involved in the processing of data which are assumed in the principles are somewhat artificial.[651]

Collection limitation principle forms the first data protection principle in the *OECD Guidelines*. It requires that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[652] The *collection limitation principle* is a cluster of three other principles: the principle of 'lawful collection', the principle of consent by the data subject and the principle that there should be some limits to the collection of personal data, which means no general license should be given, not even to certain public agencies.[653] The Explanatory Memorandum limits the *collection limitation principle* to two main aspects: limitation to the collection of data of which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive and requirements concerning data collection methods.[654] Worthwhile to keep in mind is the fact that the *Guidelines* do not include explicit principles regarding sensitive data. The reason may be the difficulty of deciding what data really are sensitive, as the assessment would differ depending on the political system, the traditions and general sentiment of a culture or a country.[655] However, reference to sensitive personal data can still be impliedly inferred in Para 2 of the *Guidelines* which says the former apply to personal data which pose a danger to privacy and individual liberties, including dangers due to the 'nature or the context' in which the data are used. Also important to keep in mind is that the *Guidelines* do not hinder the effectiveness of sensitive and non-sensitive data classification found in national laws.[656]

---

651 Ibid, 50; see also, Roos (LL.D Thesis), p.161, note 2, supra.
652 *OECD Guidelines*, Para 7.
653 Bing, p.277, note 613, supra.
654 Explanatory Memorandum 50.
655 Bing, p.278, note 613, supra.
656 Ibid.

The second principle of data protection in the *OECD Guidelines* is the *data quality principle*. The latter states that personal data which are collected should be relevant to the purpose for which they are to be use, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[657] The data quality principle has four aspects: relevancy, accuracy, completeness and up-to-dateness. All of them must be evaluated within the purpose context for which data was collected.[658] The 'purpose test' often requires the involvement of the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.[659]

The third principle is the *purpose specification principle*. This principle provides that the purposes for which personal data should be specified not later than the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.[660] As it can be noted, the purpose specification principle is directly linked to the *data quality principle* (the second principle) as well as the *use limitation principle* (the fourth principle). The *Guidelines* require as a pre-condition that the purpose for which personal data is collected must be identified. Perhaps, it is interesting to note that in contrast to all other international instruments regulating processing of personal data which are silent as to when such purpose should be identified, the *OECD Guidelines* clearly say that purpose must be identified before any data collection takes place, and in any case not later than the time of collection. Also underlined in the *Guidelines* is that later changes of purposes should also be specified before actual changes of purposes are effected.[661] Even in situations where changes from the original purposes are permitted, they are still required not to be incompatible with those original purposes and also not to be introduced arbitrarily.[662] The Explanatory Memorandum lays down a number of possibilities through which the purpose specification identification can be brought into the attention of the data subject: public declarations, information to data subjects, legislation, administrative decrees and licenses provided by supervisory bodies.[663] The *purpose specification principle* further requires that data should be destroyed (erased) or anonymised when they no longer serve the purpose for which they were collected. The reason is that control over data may

[657] *OECD Guidelines*, Para 8.
[658] Explanatory Memorandum 53.
[659] Ibid.
[660] *OECD Guidelines*, Para 9.
[661] Explanatory Memorandum 54.
[662] Ibid.
[663] Ibid.

be lost when data are no longer of interest; this may lead to risks of theft, unauthorized copying or the like.[664]

The *use limitation principle* is the fourth data protection principle. It states that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Para 9(the third principle) except: - (a) with the consent of the data subject; or (b) by the authority of the law.[665] This principle deals with uses of data that deviate the original purpose of collection. Yet, it envisages exceptions such as the consent of the data subject or his/her representative and the authority of the law including licenses granted by supervisory bodies.[666]

The *OECD Guidelines* also contains the *security safeguards principle*. The latter is the fifth principle in the *Guidelines*. Accordingly personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.[667] Yet, no absolute standard of data security is imposed by the *Guidelines* since the appropriate standard would depend upon the risks involved.[668] The *Guidelines* only requires the taking of 'reasonable' security measures. The Explanatory Memorandum 56 lists by way of examples various measures that are envisaged under the *security safeguards principle*. These include physical measures (e.g. locked doors and identification cards); organizational measures (e.g. levels with regard to access to data) and informational measures, particularly in computer systems. The Explanatory Memorandum further elaborates 'loss' of data to include cases as accidental erasure of data, destruction of data storage media and destruction of such storage media. 'Modified' is construed to cover unauthorized input of data while 'use' covers unauthorized copying.

The sixth principle is the *openness principle*. According to this principle there should be a general policy of openness about developments, practices and policies with respect to personal data.[669] Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.[670] Three criteria are laid down in this principle: establishing the existence and nature of personal data, knowing the purpose of the data controller's use of such data and obtaining the

[664] Ibid.
[665] *OECD Guidelines*, Para 10.
[666] Explanatory Memorandum 55.
[667] *OECD Guidelines*, Para 11.
[668] Bing, p.279, note 613, supra.
[669] *OECD Guidelines*, Para 12.
[670] Ibid.

identity and address of the data controller. These criteria serve realization of other rights especially those in Para 13. The Explanatory Memorandum 57 lists a number of ways (just by way of examples) how openness can be achieved in practice. These include regular information from the data controllers on a voluntary basis; publication in official registers of descriptions of activities concerned with the processing of personal data and registration with public bodies. The phrase 'readily available' is construed to mean individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling and without unreasonable cost. Yet, clearly the 'openness principle' of the *OECD Guidelines* has always been one of the weakest.[671]

The seventh principle is the *individual participation principle*. It states that an individual should have the right(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him, (i)within reasonable time, (ii) at a charge, if any, that is not excessive, (iii) in a reasonable manner and (iv) in a form that is readily intelligible; (c) to be given reasons if a request made under paragraphs (a) and (b) is denied, and to be able to challenge such denial and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.[672] Broadly, the *individual participation principle* entails a buddle of three rights: the access rights, right to reasons and the right to challenge. The access right requires generally that there should not be cumbersome procedures or unnecessary bureaucracies in gaining access to one's personal data held by data controllers.[673] Geographical distances, costs, etc should not be invoked by data controllers to deny access. In any case, response to requests for personal data by data controllers to the data subject must be made within reasonable time.[674] Upon receipt of his/her personal data, the data subject has the right to challenge their validity.[675] Through this, the data subject may require erasure, rectification, completeness or amendment.[676] The data subject has various avenues to pursue his/her challenge: through the data controller, administrative and professional bodies or courts of law depending on the laws and procedures in a member state.[677] However, this challenge cannot be leveled against the type of remedy or reliefs given as such are determined by domestic law and legal procedure.[678] With regard to the right to

[671] Kirby, p.128, note 617, supra.
[672] *OECD Guidelines*, Para 13.
[673] Explanatory Memorandum 59.
[674] Ibid.
[675] Bing, p.281, note 613, supra.
[676] Ibid.
[677] Explanatory Memorandum 61.
[678] Ibid.

reasons, this is narrowly limited to those situations where requests for information are refused.[679] In all other situations, data subjects cannot enforce their rights to be given reasons. This is one of the areas of weakness of the *OECD Guidelines*.

The eighth and last principle of data protection in the *OECD Guidelines* is the *accountability principle*. This principle requires that a data controller should be accountable for complying with measures which give effect to the principles stated above.[680] The Explanatory Memorandum 62 asserts that the obligation to comply with the data privacy principles are primarily placed over the data controllers because they are the ones who benefit from the data processing activities carried out by them. This obligation extends to service bureau personnel especially with regard to breaches of confidentiality obligations. Furthermore the accountability envisaged under the *accountability principle* does not only support legal sanctions but also compliance to the codes of conduct.

e.) Transborder Data Flows

Transborder Data Flows or simply TBDF is broadly defined as the electronic movement of data between countries.[681] As pointed out, regulation of the movement of personal data following the development of computer technology had posed challenges to the continued sustainability of the objectives for which OECD was established.[682] To address those challenges the *OECD Guidelines* introduced four main principles in Part three under the name 'basic principles of international application: free flow and legitimate restrictions.'

Para 15 of the *Guidelines* obliges member countries to take into consideration the implications for other member countries of domestic processing and re-export of personal data. This is expressed in the Explanatory Memorandum as 'respect by Member countries for each other's interest in processing personal data and individual liberties of their nationals and residents.'[683] The

---

679 Explanatory Memorandum 60.
680 *OECD Guidelines*, Para 14.
681 Fishman, W.L., Introduction to Transborder Data Flows', Stanford Journal of International Law, 1980, Vol16, pp.1-26, at p. 1.
682 For detailed discussion about the impediments to international harmonisation of data privacy laws see, Kirby, M., 'Information Security-OECD Initiatives', Journal of Law and Information Science, 1992, Vol.3, No.1, pp.25-46, at pp.27-30. This article is also available in The Computer Law and Security Report, 1992, Vol. 8, No.3, pp. 102-110, at pp. 102-104. Also important to keep in mind, the 'Information Security-OECD Initiatives' first appeared as a paper presentation in the Japan Information Processing Development Centre: International Symposium of Information security, Tokyo, Japan, 17 October 1991; see also, Cooper, D.M., 'Transborder Data Flow and the Protection of Privacy: The Harmonization of Data Protection Law', Fletcher Forum, 1984, Vol.8, No.2, pp.335-352.
683 Explanatory Memorandum 63.

obligations imposed by Para 15 are geared towards cubing liberal policies which are contrary to the spirit of the *Guidelines* and which attempt to circumvent or violate protective legislation of other member countries.[684] Also the need to respect envisaged in Para 15 carries with it an obligation to support each other's efforts to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of personal data where control is slack or non-existent.[685] Para 16 obliges member states to take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure i.e. protected against unauthorized access, loss of data and similar events.[686] Para 17 permits restrictions to TBDF subject to four conditions: where a member state to where data is to be transferred does not yet substantially observe these *Guidelines*; where re-export of such data would circumvent its domestic privacy legislation; where regulation of certain categories of personal data is required and the same is supported by domestic privacy regulations and where the other member country does not provide 'equivalent protection'. Para 18 urges member states to avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection. This paragraph ensures that a meaningful balance between privacy protection interests and TBDF is achieved.[687]

Worthwhile to keep in mind, the *Guidelines* do not explicitly address the issue of conflict of laws and jurisdiction. The only reference to the issue is found in the *Guidelines*, in which member countries agree to work towards the development of principles to govern the applicable law in cases of transborder data traffic.[688]

f.) National Implementation

As pointed out, the *OECD Guidelines* are not legally binding on member states. Nevertheless, the members of the OECD consider to be practically binding, demonstrated by their adoption with reservations by certain countries-an act which might otherwise be thought superfluous for a non-

[684] Ibid, 64.
[685] Ibid.
[686] Ibid, 66.
[687] Ibid, 68.
[688] *OECD Guidelines*, Para 22; Explanatory Memorandums 74, 75 and 76; OECD Declaration on Transborder Data Flows 1985(Adopted on 11 April 1985); see also Bing, p.284, note 613, supra.

binding instrument.[689] In this way, the practical significance of the *Guidelines* on member states depends on the level of details of implementation by such members. The implementation of the *Guidelines* may take various forms ranging from the adoption of data privacy legislation to self-regulations.[690] Those instruments must provide adequate sanctions and remedies as well as ensure that there is no unfair discrimination against data subjects.[691] Also in implementing the *Guidelines* at national level, member states are encouraged to set up supervisory authorities, rely on courts, public authorities or already established facilities to enforce the privacy laws.[692] Part and parcel of the duties of these bodies are to provide advice to data controllers, give them legal aid and resolve complaints and disputes.[693]

g.) International Cooperation

To ensure collectivism in implementing the *OECD Guidelines* Para 20 urges member states to exchange information upon request regarding observance of principles set out in the *Guidelines*. In order to facilitate such exchange of information member states are also urged to establish procedures for such purposes.[694]

Final points should be made with regard to the *OECD Guidelines*. The most important is that for the past thirty years the *Guidelines* have been influential in the adoption of data protection legislation within OECD and beyond. Australia, New Zealand, Japan serve as non-exhaustive list of countries which have been influenced by the *OECD Guidelines* in adopting data privacy legislation. Another illustration of such influence which deserves mention here is the Asia-Pacific Privacy Framework 2004 or APEC Privacy Framework (see 3.3.3). Though of course there are still significant departures from the *Guidelines,* the APEC Privacy Framework owes much to the former.[695] However with the rapid development of technologies in the past thirty years, the *Guidelines* have been made practically difficult to implement. Michael Kirby, the chairperson of the Expert Group which formulated the *Guidelines* has in several occasions openly made

689 Bing, p.284, note 613, supra.
690 *OECD Guidelines*, Para 19; Explanatory Memorandums 69 and 70.
691 Ibid.
692 Ibid.
693 Ibid.
694 *OECD Guidelines*, Para 21; Explanatory Memorandums 71, 72 and 73.
695 Greenleaf, note 560, supra; see also, Greenleaf G., 'The APEC Privacy Initiative:"OECD Lite" for the Asia-Pacific?', Privacy Laws & Business, 2004, Vol.71, pp. 16-18; Greenleaf, G., 'Asia-Pacific Data Privacy: 2011, Year of Revolution? University of New South Wales, Faculty of Law Research Series, 2011, Paper No.29, pp.1-17.

admission to this difficult.[696] To illustrate some of the issues repeatedly raised by Kirby are the application of the *use limitation principle* and the *purpose specification principle*. He has noted for instance, that, social networks have arisen in the past ten years. That has raised challenges in use limitation and purpose specification. The notion of 'consent' has also been challenged with the new technology not envisaged by the Expert Group.

3.3.1.5 CoE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981

The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981(*ETS 108* or *Convention 108*) was adopted by the Council of Europe in response to the growing volume of automatic processing of personal data as a consequence of advancements in information technology and means of keeping and processing information in digital forms.[697] The *Convention 108* was open for signature on 28 January 1981 and officially entered into force on 1 October 1985. Currently forty-three out of forty-seven Council of Europe countries are a party to the Treaty and three others have signed it.[698] States outside of the Council of Europe can be invited to accede to the *Convention 108*.[699] Undoubtedly, it is because of this and certainly to better underline the ample scope of accession to the *Convention* by non-European states the instrument's title is described as 'Convention' as opposed to 'European Convention.'[700] Yet, the accession clause in the *Convention* does not envisage accession by developing countries including those from African continent but rather the non-European member countries to the OECD as clearly stated in Explanatory Report 90.[701]

---

[696] Kirby, p.12, note 611, supra; Information and Privacy Commissioner/Ontario., 'Should the OECD Guidelines Apply to Personal Data Online?', A Report to the 22nd International Conference of Data Protection Commissioners, Venice, Italy, September 2000.

[697] Neuwirt, K., 'Acceso a la información y protección de datos personales: dos caras de un mismo derecho-2 Seminario Internationacional, Connvention 108: New Challenges for Data Protection in Non-European States', 13-14 November 2008, Mexico City, http://www.infodf.org.mx/web/participantes/neuwirt/Abstract%20Karel%20Neuwirt.pdf last visited 26/12/2011.

[698] Greenleaf, G., 'Graham Greenleaf's Global Table of Privacy Law', as at 10 November 2011, http://www2.austlii.edu.au/~graham/DP_Table/DP_TABLE.html last visited 26/12/2011; see also, Greenleaf, G., 'The Global Trajectory of Data Privacy Laws', SCRIPT Seminar, Edinburgh, 8 December 2011, pp.1-13, at p.8; Greenleaf, p.15, note 572, supra; Bygrave, p.20, note 503, supra.

[699] *Convention 108*, Art 23.

[700] Explanatory Report to *CoE Convention* 108 (hereinafter Explanatory Report), 24. Yet in broadening the scope of Art 23 of the *Convention 108*, the Council of Europe had to amend the *Convention* in 1999 to allow the European Communities to accede as prior the former envisaged accession by states only (Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 15 June 1999).

[701] Explanatory Report 90 states, 'The Convention is destined to be an "open" one with a wide geographic scope (see paragraphs 14 and 15). The Convention was elaborated in close co-operation with OECD and the non-European member countries of that organisation and it is in particular those countries which one had in mind when this article was drafted.' See also the recent Resolution of the Parliamentary Assembly of the Council of Europe,

Historically, the *Convention 108* traces its origins from two Council of Europe Resolutions of the Committee of Ministers: Resolution (73) 22 on the Protection of Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector 1973[702] and Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector 1974.[703] Compared to the OECD in this context, the European Council seems to have started taking serious efforts towards regulation of processing of personal data much earlier. Yet, it was not until 1981 when the *Contention* was signed only one year after the *OECD Guidelines* were adopted.

The circumstances which necessitated the Council of Europe to adopt specific regulations for processing personal data at that time can be explained in the deficiencies of privacy protection in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) 1950. First, it was clear that the ECHR applies to relations between individuals and public authorities and not those of private parties *inter se*, e.g. an insurance company.[704] Second, it was also revealed that the ECHR protects two fundamental rights in the field of information which may conflict each other: the right to respect of one's private life and family (Art 8) and the right to freedom of information (Art10).[705] The *Convention* does not say where the balance should be struck.[706] Third, the potential for computer abuse covers a much broader range than the *Convention's* protection against the right to privacy.[707] Apart from the deficiencies in the ECHR, it was also apparent to the Council of Europe that many of its member states had no adequate laws for protection of personal data.[708] To address those challenges in the context of the rapid development of technology, adoption of general principles of protection of personal data was the only viable option. Also important to note is the fact that cross-border transfer of personal data catalyzed the need of adopting common rules that would harmonise the level of protection of personal data across member states.

Resolution 1833(2011) on the Activities of the OECD partly aiming at promoting wide accession to the *Convention 108* by OECD countries especially those which are non-European states.

[702] Adopted by the Committee of Ministers on 26 September 1973 at the 224th Meeting of the Ministers' Deputies.

[703] Adopted by the Committee of Ministers on 20 September 1974 at the 236th Meeting of the Ministers' Deputies.

[704] Hondius, F.W., 'Data Law in Europe', Stanford Journal of International Law, 1980, Vol.16, pp.87-111, at p. 92.

[705] Ibid.

[706] Ibid.

[707] Ibid.

[708] Bygrave, note 698, supra.

a) Philosophical Basis

The Council of Europe has traditionally been a human rights organization, though it has moved into such areas as social welfare and penal legislation.[709] The organization has even a Committee on Legal Data Processing, which is mainly concerned with legal information services.[710] As already explained, the objectives for which the Council of Europe came to be established were largely influenced by abuses of human dignity during the World War II. Such abuses were facilitated by misuse of personal information. To address the traumas of the War, the Council of Europe became established to foster co-operation among European countries in the areas of legal standards, human rights, democratic development, the rule of law and cultural cooperation. Regulation of personal data processing is just one of such areas that fall within the competence of the Council of Europe. In such context and in contrast to the *OECD Guidelines*, the preamble to the *Convention 108* reaffirms the value of human rights protection and fundamental freedoms of the individuals as the basis upon which it was developed. Hence the *Convention* focuses on the human rights aspects of the traditional privacy concept.[711]

b) Structure and Nature

Structurally, the *Convention 108* comprises the preamble of four recitals and seven chapters with twenty seven articles. The latter stipulate the substantive law provisions in the form of basic principles, special rules on transborder data flows and mechanisms for mutual assistance and consultation between the parties.[712] The *Convention* has been amended once since it came into force to accommodate the accession of the European Union.[713] Also important to note is that it has one Protocol [714](Additional Protocol or Protocol) which has to be read in conjunction with the former. Moreover, since its adoption, fourteen sector specific Recommendations have been issued under the *Convention* in an attempt to partly respond to the uniqueness of different sectors and challenges of technologies that came subsequently.[715] While these recommendations are not

[709] Bing, note 613, supra.
[710] Ibid.
[711] Ibid.
[712] Explanatory Report 18.
[713] See note 700, supra.
[714] Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, ETS No.181, Strasbourg, 8.XI.2001.
[715] Recommendation No.R (81) 1 on regulations for automated medical data banks (23 January 1981) [replaced by Recommendation No. R (97) 5]; Recommendation No.R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983) [replaced by Recommendation No. R(97) 18 with regard to statistics]; Recommendation No.R(85) 20 on the protection of personal data used for the purposes of direct

strictly binding in a legal sense, they carry considerable weight when the various detailed regulations are prepared.[716] Thus, they supplement and amplify the rules of the *Convention*.[717] Apart from the above, there is also the Explanatory Report to the *Convention* similar to the Explanatory Memorandum to the *OECD Guidelines*. Although it does not constitute an instrument providing an authoritative interpretation of the text of the *Convention* it facilitates the understanding of the provisions contained in it.[718] The Explanatory Report itself has ninety three paragraphs structured in such nature as to provide background information to the adoption of the *Convention* and interpretation of its provisions.

In contrast to the *OECD Guidelines*, the *Convention 108* is a legally binding international treaty concerning data protection issues. Yet, it does not provide, of itself, as set of rights directly enforceable in national courts rather it requires contracting states to incorporate its principles in their domestic legislation to become enforceable.[719] As such, it exerts more force on its members and has since influenced the adoption of the Directive 95/46/EC in the European Union and beyond as amply demonstrated at the 33rd international conference of data protection and privacy commissioners, Mexico City, 2-3 November 2011 where the Council of Europe pointed to its data protection as the global standard.[720]

c) Objectives and Scope

The object and purpose of the *Convention 108* is set out in Art 1. The same is formulated in broad terms as 'to secure in the territory of each Party for every individual, whatever of his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to

marketing (25 October 1985); Recommendation No.R(86) 1 on the protection of personal data for social security purposes (23 January 1986); Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987); Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (18 January 1989); Recommendation No.R(90) 19 on the protection of personal data used for payment and other operations (13 September 1990); Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991); Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995); Recommendation No.R(97) 5 on the protection of medical data (13 February 1997); Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997); Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999); Recommendation No.R(2002) 9 on the protection of personal data collected and processed for insurance purposes (18 September 2002); Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010).

716 Selmer, K.N., 'Council of Europe Convention on Automatic Data Processing', Medical Informatics, 1989, Vol.14, No.3, pp.211-214, at p.212; see also Bygrave, p.25, note 503, supra.

717 Selmer, note 716, supra.

718 See the introductory remarks II to the Explanatory Report.

719 Explanatory Report 38 and 60; see also Bygrave, p.22, note 503, supra.

720 News, Council of Europe-Data Protection Home Page, http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp last visited 28/12/2011.

privacy, with regard to automatic processing of personal data relating to him otherwise known as data protection'. As it can be noted from this provision, the *Convention* aims to set standards for data protection at the national level.[721] The expression 'whatever of his nationality or residence' means that any restrictions in the national legislation by member states conferring rights to individuals on accounts of their nationality or legally resident aliens shall be regarded as incompatible to the spirit of the *Convention*.[722] Consequently this requirement extends the scope of the *Convention* to every individual.[723] However, apart from seeking to set standards for data protection at the national level, the *Convention* also sets standards that ensure the free flow of information across member states is not unnecessarily interrupted.[724] This second aim intends further to prevent states from adopting such policies as economic protectionism.[725]

The above objectives and purpose delineate the scope of the *Convention* in both broad and restrictive terms. Art 3 (1) of the *Convention* states, 'the Parties undertake to apply this *Convention* to automated personal data files and automatic processing of personal data in the public and private sectors.' In its broad scope the *Convention* binds both the public and private sectors. However it avoids repeating this requirement in the other provisions partly because these terms may have a different meaning in different countries.[726] Also the deliberate omission to use the public-private dichotomy approach in the other provisions of the *Convention* plays the role in the declarations which the parties may make with regard to its scope.[727] Yet, in its restrictive sense the *Convention* applies only to 'automated data file'. By 'automated data file' it means any set of data undergoing 'automatic processing'.[728] The latter concept (i.e. automatic processing) includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.[729] However with the exceptions of Arts 5(a) and 12, the collection of information falls outside the notion of 'processing'.[730] Also important to keep in mind is that both concepts 'automated data file' and 'automatic processing' must be linked to two other

[721] Roos, (LL.D Thesis), p.178, note 2, supra.
[722] Explanatory Report 26.
[723] For contrary approach see e.g., Kusamotu, note 165, supra.
[724] *Convention 108*, Art 12(2); see also Explanatory Report 62 which states, 'The aim of this article is to reconcile the requirements of effective data protection with the principle of free flow of information, regardless of frontiers, which is enshrined in Article 10 of the European Human Rights Convention.'
[725] Explanatory Report 25 partly states, '...It is also underlined that the Convention should not be interpreted as a means to erect non-tariff barriers to international trade ....'
[726] Explanatory Report 33.
[727] Ibid.
[728] *Convention 108*, Art 2(b).
[729] Ibid, Art 2(c).
[730] Explanatory Report 31.

concepts 'personal data' and 'controller of the file' in order to assign their proper interpretation. The former means any information relating to an identified or identifiable individual otherwise known as 'data subject'.[731] The notion 'identifiable individual' in this definition means a person who can be easily identified: it does not cover identification of persons by means of very sophisticated methods.[732] However this definition is problematic. First, it is practically difficult to assess the 'easy' with which identification can be made as this varies relatively from one data controller to another. Second but somewhat linked to the first reason is that the level of sophistication of methods is also dependant on the means (e.g. technology) and resources available to each data controller. As to 'controller of file' it means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.[733]

Worthwhile to keep in mind is that *Convention 108* permits states to undertake exceptions in their national legislation. Such exceptions have the effect of narrowing the broad scope considered above. At the same time the exceptions may broaden the restrictive scope already considered. For example, while in its restrictive sense the *Convention* seems to apply on natural person data subjects, states are also permitted to stipulate provisions in their laws which extend such application to legal entities or what are also known as juristic persons.[734] Also, states may provide in their national legislation that manual files or files which are not processed automatically shall be covered.[735] States may further exclude application of the *Convention* to certain categories of automated data files provided a list of such categories shall be deposited.[736] The latter must only constitute categories of data files which are not or not yet subject to data protection legislation domestically.[737] Also important to note is the broad range of ambit in Art 11 of the *Convention* which categorically states, 'none of the provisions of this chapter(Chapter II-Basic Principles for Data Protection) shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in the Convention.' It is arguable that Art 11 is limited to the extent of the application of the provisions of Chapter II of the *Convention* and does not in any way stipulate beyond the general scope of the *Convention* in Art

731 *Convention 108*, Art 2 (a).
732 Explanatory Report 28.
733 *Convention 108*, Art 3(d). Note that the term 'controller of the file' is used synonymously with the term 'controller' in Art 2(d) of the Directive 95/46/EC and in most national data protection legislation. Find detailed discussion about these terminologies in 2.2 of this thesis.
734 *Convention 108*, Art 3(2), (b).
735 Ibid, 3(2),(c).
736 Ibid, 3(2),(a).
737 Explanatory Report 34.

3, otherwise to read the former as exceeding the ambit of the latter is to invite internal conflicts of the provisions of the *Convention*.

d) Data Protection Principles

The *Convention* contains eight data protection principles similar to those enshrined in the *OECD Guidelines*. While some of such principles are explicitly stated in the *Convention* others may only be implied in other formulations.

The first data protection principle is the *fair and lawful processing*. The principle stipulates that personal data 'shall be obtained and processed fairly and lawfully.'[738] The basic criteria underlying this principle are 'fairness' and 'lawfulness'. While the former term may be difficult to determine it may roughly be examined based on a number of other criteria such as whether the processing involves a legitimate reason for doing that; whether the processing of personal data is in itself transparent; whether data was obtained without coercing the data subject or by using trickery means unknown to the data subject; abstinence from re-using personal data for purposes other than those specified during data collection.[739] The list given here is not exhaustive rather it serves as examples of what envisages 'fairness'. The 'lawfulness' criterion presupposes authorization of the data protection process by law or consent from the data subject.

The second principle is the *purpose specification*. The latter requires that personal data 'shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.'[740] There are three basic criteria in this principle: specific and legitimate purpose as well as compatible use. Reference to 'purpose' in this principle indicates that data controllers should not be allowed to store data for undefined purposes.[741] The *Convention* leaves in the mandate of states to specify the different ways in which the legitimate purpose should be formulated in their national legislation.[742] Interestingly, it does not include any explicit reference nor contain a specific principle limiting the dissemination of data, although an implicit limitation may be derived from the expression '…not used in a way incompatible with those purposes.'[743]

---

738 *Convention 108*, Art 5(a).
739 Bygrave, note 542, supra.
740 *Convention 108*, Art 5(b).
741 Explantory Report 41.
742 Ibid.
743 See also, Bing, note 668, supra.

The third principle is *minimality*. It requires that personal data 'shall be adequate, relevant and not excessive in relation to the purposes for which they are stored.'[744] The *minimality* principle is further amplified by the other requirement that personal data 'shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.'[745] Yet the Explanatory Report interprets the time-limits requirement for the storage of data in their name-linked form does not mean that data should after some time be irrevocably separated from the name of the person to whom they relate, but only that it should not be possible to link readily the data and the identifiers.[746] It is submitted that, although this requirement requires anonymization of data, it is highly possible to re-link the names to their respective identifier at a later stage. This possibility is exacerbated by the fact that the separation between the names and their corresponding identifiers only needs to be made in such a away that it is not quickly and without difficulty to link them.

The fourth principle is the *adequate information quality*. It states that personal data 'shall be adequate, accurate and relevant in relation to the purposes for which they were processed.'[747] By limiting processing of personal data to what is adequate, accurate and relevant to achieve a specified purpose, the *adequacy information quality* plays a significant role in facilitating the functioning of others principles such as the *fair and lawful processing*, *purpose specification* and *minimality*.

The fifth principle is s*ensitivity*. According to this principle, personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards.[748] The same shall apply to personal data relating to criminal convictions.[749] While the risk that data processing is harmful to persons generally depends not on the contents of data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests.[750] It is these categories that are envisaged in the s*ensitivity* principle. However, it is important to underline that the expression *'revealing…political opinions, religious or other beliefs'* covers also activities

[744] *Convention 108*, Art 5(c).
[745] Ibid, Art 5(e).
[746] Explanatory Report 42.
[747] *Convention 108*, Art 5(c) and (d).
[748] Ibid, Art 6.
[749] Ibid.
[750] Explanatory Report 43.

resulting from such opinions or beliefs.[751] Also important to note is the term 'personal data concerning health' which includes information concerning the past, present and future, physical or mental health of an individual.[752] Such information may relate to a person who is sick, healthy or deceased.[753] Reference to the expression 'domestic law' has to be understood in its wide sense including but not limited to legislation, specific regulations, and administrative directives as long as the necessary level of protection is secured.[754] Worthwhile to keep in mind 'criminal conviction' in the sense of the s*ensitivity* principle should be understood as convictions based on criminal law and the framework of a criminal procedure.[755]

The sixth principle is *data security*. The principle states that appropriate security measures shall be taken for the protection of data stored in automated data files against accidental, unauthorized destruction, accidental loss as well as against unauthorized access, alteration or dissemination.[756] This principle seeks to prevent unauthorized access to the automated data file as well as cases of accidental distortion. The security measures envisaged in the *data security* principle must be adapted to the specific function of the file and the risks involved.[757] Moreover they should be based on the current state of the art of data security methods and techniques in the field of data processing.[758] The problem that is likely to arise in the implementation of this provision is how to determine whether such methods reflect the current state of the art of the data security and techniques in the field of data processing.

The seventh principle is *transparency*. The latter states that any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file.[759] At the same time such person shall be enabled to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form.[760]

---

[751] Ibid, 44.
[752] Ibid, 45.
[753] Ibid.
[754] Ibid, 46.
[755] Ibid, 47.
[756] *Convention 108*, Art 7.
[757] Explanatory Report 49.
[758] Ibid.
[759] *Convention 108*, Art 8(a).
[760] Ibid, Art 8(b).

The eighth principle is *rectification*. It states that any personal shall be enabled to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of the Convention.[761] Also such person shall be enabled to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs 8(a) and 8(b) of Article 8 is not complied with.[762]

As it can be noted, the operation of the *transparency* and *rectifications* principles depends on each other. This is because both are designed to enable a data subject to defend his rights vis-à-vis automated data files.[763] In essence, transparency facilitates the realization of the rectification rights.

It is important to underline that the functioning of the above principles is subject to certain exceptions and restrictions provided under the *Convention*. More specifically, departures from those principles are permitted so long states meet the criteria set out in Arts 9 and 11. The former state that derogations from the provisions of Articles 5, 6 and 8 of the Convention shall be allowed when such derogation is provided for by the law of the part and constitutes a necessary measure in a democratic society in the interests of: (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offence; (b) protecting the data subject or the rights and freedoms of others. The derogations in Art 11 have already been considered in 3.3.1.5 (c) above.

Criticizing the effectiveness of the above data protection principles contained in Chapter II of the *Convention,* Lee A. Bygrave argues:-

> 'The Chapter II principles are formulated in general, abstract way and many key words are left undefined-also by the *Convention's* Explanatory Report. While this has certain advantages, the diffuseness of the principles detracts from their ability to harmonise the laws of the contracting states. This weakness is exacerbated by the Convention otherwise permitting discretionary derogation on numerous significant points (see, for example, Articles 3,6 and 9). This, in turn, has undermined the ability of the Convention to guarantee

761 Ibid, Art 8(c).
762 Ibid, Art 8(d).
763 Explanatory Report 50.

> the free flow of personal data across national borders. At the same time, the abstract nature of the principles undercuts their ability to function as practical "rules for the road" in concrete situations.'[764]

Despite the above criticisms, the *Convention 108* remains the legally binding international treaty which has influenced adoption of data privacy legislation within and outside of Europe.

e.) Transborder Data Flows

As pointed out, ensuring free flow of personal data across member states remains one of the primary object and purpose of the *Convention*. To ensure there is cross-jurisdictional free flow of personal information, the *Convention* incorporates a number of principles in Art 12. The basic rule here is that a state party shall not restrict flows of personal data to the territory of another state party unless the latter fails to provide 'equivalent protection' for the data.[765] A major gap in Chapter III of the *Convention* is the absence of rules of flow of personal data from a party to non-party state.[766] In 2001, the Council of Europe remedied the anomaly by adopting an Additional Protocol[767] which incorporates in its Art 2 provisions on data flow from party to non-party states similar to those found in the Directive 95/46/EC.[768] It is interesting to note that the *Convention* applies different criteria in the transfer of personal data across countries. The first criterion is the 'equivalent protection' in Art 12 of the *Convention* while the second is the 'adequate level of protection' provided in Art 2 of the *Convention's* Additional Protocol. The former is invoked when the transfer of personal data is concerning inter-parties to the *Convention* while the latter applies when transfer of personal data involves a party and a non-party state to the *Convention*. Arguably this is a weakness to the *Convention* and may still raise questions as to whether the Council of Europe intends to facilitate economic protectionism policies against non-party states.

Also important to keep in mind is that neither the *Convention* nor its Protocol contains choice of law rules. This is similar to what befall the *OECD Guidelines*. However the omission is mitigated somewhat by the provision in Chapter V for establishing a Consultative Committee which is

[764] Bygrave, note 716, supra.
[765] Bygrave, p.23, note 503, supra.
[766] Ibid.
[767] See note 714, supra.
[768] Bygrave, pp.23-24, note 503, supra.

charged with developing proposals to improve application of the *Convention.*[769] Yet at present no any concrete choice of law rules have ever been developed by this body.

f.) National Implementation

When the *Convention 108* was originally adopted, it did not provide how at the national level it would be supervised. This omission left states to adopt different strategies which in the long run risked the harmonization of data protection legislation across member states. To remedy the situation in 2001, the Council of Europe incorporated in the *Convention's* Protocol specific provisions regarding supervisory authorities.[770] Yet such provisions fall short of mandating that each contracting state establish a special control body in the form of a data protection authority or the like.[771] Also they fail to specify minimum requirements regarding the competence and independence of each authority.[772]

g.) International Cooperation

Articles 13-17 of the *Convention* regulate international cooperation. To facilitate such cooperation each party is required to designate the authority and its competence.[773] In this cooperation parties may at requests of each other supply information on law and administrative practices in the field of data protection.[774] Moreover, each party is obliged to assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Art 8 of the *Convention*.[775]

In conclusion, it is important to point that when the *Convention* was adopted, the computer was not as it is today. Moreover, the subsequent rise in the Internet in the 1990s brought profound challenges to issues of data protection. After thirty years of being in force several challenges have occurred which make the implementation of the *Convention* practically difficulty especially in the areas of technology. The Council of Europe is currently engaging in a process of revising its

[769] Ibid, p.24.
[770] Additional Protocol, Art 2.
[771] Bygrave, note 769.
[772] Ibid.
[773] *Convention 108*, Art 13(2).
[774] Ibid, Art 13(3).
[775] Ibid, Art 14(1).

Data Protection Convention to meet and overcome these challenges.[776] However while the *Convention* is being overhauled the review aims at 'modernizing' the *Convention* without altering its basic principles, but looking at adding new ones such as those of proportionality and privacy by design.[777] The review process is set to end in 2012. While it is too early to predict the contents of the final draft of the 'modernized' *Convention 108*, it is important to underline that based on the submission of comments to the Expert Committee most of the pitfalls highlighted above have been widely commented. It is interesting to note that Lee A. Bygrave whose above critics to the *Convention* are most appealing have had opportunity to be onboard of the review process under the CSLR.

3.3.1.6 European Directive on Protection of Personal Data 1995

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, commonly cited as Directive 95/46/EC; sets comprehensive regulations for protection of personal data in the European Union. It officially came into force on 24 October 1998, the last date given to member states to transpose the law into their domestic legal systems.[778] Also important to bear in mind is that the Directive has been incorporated into the 1992 Agreement on the European Economic Area (EEA) such that states which are not EU members but are party to the EEA Agreement (i.e. Norway, Iceland and Liechtenstein) are legally bound by the Directive.[779]

The adoption of the Directive was largely attributed by the deficiencies in the Council of Europe *Convention 108/1981*. Peter Blume asserts that the purpose of the *Convention* is the promotion of

---

[776] See, Comments submitted by the Computer Law and Security Review(CLSR) together with the International Association of IT Lawyers(IAITL) and the Institute for Law and the Web(ILAWS) in response to the Expert Committee's public on the document titled 'BEFORE THE EXPERT COMMITTEE SET UP UNDER THE CONVENTION 108: MODERNISATION OF CONVENTION 108', p.1., http://www.soton.ac.uk/ilaws/newsandevents/2011/CONVENTION_108-CLSR.pdf last visited 29/12/2011; see also European Privacy Association(EPA), 'FEEDBACK TO THE MODERNISATION OF CONVENTION 108', http://www.europeanprivacyassociation.eu/public/news/Contribution%20-%20Modernisation%20108%20-%20final%20for%20EPA%20and%20%20APEP.pdf last visited 29/12/2011; CoE, 'THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA: MODERNISATION OF CONVENTION 108 PROPOSALS', T-PD-BUR(2011)27_en, Strasbourg, 15 November 2011, http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD-BUR_2011_27_en.pdf last visited 29/12/2011.

[777] Ibid, (CLRL),(IAITL),(ILAWS).

[778] Directive 95/46/EC, Art 32.

[779] Bygrave, p.31, note 503, supra.

transborder data flow on the basis of equivalent levels of protection in the different countries. [780] For many reasons this purpose has not been fulfilled to a satisfactory extent, and as personal information has become more and more internationalized, the necessity of more efficient legal instruments has become clearer. Accordingly, the adoption of Directive 95/46/EC was just a step in that direction. Blume's assertion finds support of Charles Raab and Colin Bennett, who, in their joint article observe:-

> 'However, practice has revealed several drawbacks to the Convention itself as an adequate basis for protecting privacy across borders. Many questions about definition and scope have taxed the minds of data protectors. Divergences among countries in the enactment and implementation of common principles, as well as uncertainties about which country's jurisdiction should apply in particular instances, increasingly present problems for international activity. In general, then, however influential the Convention has been, it has not effected a closer harmonization in practice amongst ratifying countries.'[781]

The correctness of the above assertions is reflected in the Directive's own provisions which state, 'the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in the Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Data Processing of Personal Data.'[782] Yet, harmonization problems pinpointed in the preceding paragraphs need not be exaggerated. The reason is that even after the adoption of the Directive 95/46/EC such problems have never been resolved as empirically observed by Karen McCullagh who argues that although the Directive aimed at promoting harmonization of data protection within EU, preliminary findings suggest that such aim remains much more apparent than real.[783] It is largely because of this that the Directive is in the reform of being overhauled and replaced by the Regulation of the European Parliament and the Council on the protection of individuals with regard to the free movement of such data (General Data Protection Regulation).[784] Subsequent reference to this instrument shall be Regulation or GDPR

---

[780] Blume, P., 'Privacy as a Theoretical and Practical Concept', International Review of Law Computers & Technology, 1997, Vol.11, No.2, pp.193-202, at p.199.
[781] Raab, C.D and Bennett, C.J., 'Protecting Privacy across Borders: European Policies and Prospects', Public Administration, 1994, Vol.72, pp.95-112, at pp.101-102.
[782] Directive 95/46/EC, Recital 11.
[783] McCullagh, note 499, supra.
[784] Note that this instrument is still a work in progress. In December 2011 the researcher got the final draft of the proposed law which was leaked to the press in the beginning of December 2011 prior to its official publication by

to ease citation. Yet, despite the proposed reform of the European data protection law, this thesis proceeds to offer a detailed discussion of the Directive and only a general discussion of the Regulation for the following reasons:-

First, although the Directive is proposed to be repealed by the Regulation, the latter law retains most of the general principles of data protection in the former. Hence the case law developed by the ECJ on the Directive and other practices by Data Protection Authorities in member states continue to be relevant. Second, it will take sometime for the Regulation to be formerly put in practice. Initially it was proposed that the Regulation would come into force in 2014. However, it is unlikely for the new law to be operational at that date as the Regulation is still under intense debate by EU member states.Because of this, any detailed and deeper analysis of the Regulation at this stage is pre-mature as the practice of the law is yet to be observed. Third, since the Regulation came about as a result of the mischief which befell the Directive, it is likely that in the implementation and interpretation of the former the latter law be considered as the starting point. Fourth, during transition period, the Directive will continue to be in force.

In order to maintain focus, the Directive is considered first then the Regulation follows. This helps to appreciate the problems and challenges which necessitated the repeal of the former law. Also, it facilitates to clearly understand the proposed law: what is proposed, what has been retained, and what has been discarded.

a.) Philosophical Basis

Like the Council of Europe *Convention 108*, Directive 95/46/EC has its foundation in the human rights treaties and national constitutions of member states. This is reflected in various recitals of the preamble to the Directive which frequently refer to the European Convention for the Protection of Human Rights and Fundamental Freedoms for its normative base.[785] Moreover the philosophical basis of the Directive in the human rights can further be derived from the object and purpose clause in Art 1(see 3.3.1.6 c).

---

the European Commission; see Version 56 of 29/11/2011; see also, Linkomises, L., 'EU regulation planned to harmonise national laws', Privacy Laws & Business International Report, 2011, No. 114, pp. 1, 3-4.

[785] See, e.g., Directive 95/46/EC, Recitals 1, 2,3,10,33,34,37.

b.) Structure and Nature

Compared to *Convention 108* and *OECD Guidelines*, the Directive is the longest and more detailed text. The latter has a preamble of seventy two recitals. Its substantive provisions are contained in seven chapters comprising a total number of thirty four articles. The length of details contained in the preamble has served as a reference point in making interpretation of the substantive provisions of the Directive.[786] The Directive lacks explanatory memorandum or report similar to those accompanying the *Convention* and the *Guidelines*. As a result the *travaux préparatoires* to the Directive have served significant role as interpretation references.

Directive 95/46/EC is a legally binding instrument just like the *Convention 108*. Hoewver, to amplify its binding character, the Directive is enforceable at the European Court of Justice (ECJ). Although in this case the ECJ's jurisdiction is limited to determination of references by member states for preliminary rulings, it has given the Directive a far greater margin of its enforcement compared to the *Convention*.[787]

c.) Objectives and Scope

The Directive has two objectives. First, is to 'protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.'[788] The second objective of the Directive is to promote free flow of personal data within the European Union.[789] It is formulated in the negative, 'member states shall neither restrict nor prohibit the free flow of personal data between member states for reasons connected with the protection afforded under paragraph one.'[790] Reference to 'the protection afforded under paragraph 1' means that member states should not impede the free flow of personal data by advancing reasons related to implementation of the first objective. The second objective appears

---

[786] It is interesting to note that in the English common law legal system preambles to constitutions are not considered as part and parcel of the substantive provisions of such constitutions unless expressly provided to the contrary (see e.g., notes 126,128,129,130,131 and 132, supra). Hence courts do not rely on such preambles as interpretative aids to constitutions.

[787] A preliminary ruling is a decision of the European Court of Justice (ECJ) on the interpretation of European Union law, made at the request of a court of a European Union member state. The name is somewhat of a misnomer in that preliminary rulings are not subject to a final determination of the matters in question, but are in fact final determinations of the law in question. Preliminary rulings can also be made, in certain circumstances, by the European General Court, although most are made by the ECJ, http://en.wikipedia.org/wiki/Preliminary_ruling last visited 30/12/2011.

[788] Directive 95/46/EC, Art 1(1).

[789] Ibid, Art 1(2).

[790] Ibid.

to outweigh the first. In any case it serves to offer evidence that the Directive is ultimately concerned with realizing the effective functioning of the EU's internal market, and only secondarily with human rights.[791]

Similar to the *OECD Guidelines* but contrary to *Convention 108*, the initial scope of application of the Directive is broad. First, it applies to processing of personal data in both public and private sectors.[792] Yet, it does not apply in public sector on matters falling outside the Community law[793] such as those relating to processing of personal data in the context of public security, defence, state security and the activities of the state in areas of criminal law.[794] Also, the Directive excludes its application from the domain of the private sector involving processing of personal data by a natural person in the course of a purely personal or household activity.[795] The expression 'in the course of purely personal or household activity' was interpreted by the ICJ in *Lindqvist*[796] to mean the processing of personal data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding records of addresses but does not include say, for example, publication on the Internet so that those data are made accessible to an indefinite number of people.[797]

Apart from the public-private coverage, the Directive applies to both automatic and manual processing of personal data.[798] However, it limits this scope to the structured 'filing systems' excluding unstructured and any other categories of manual files.[799] By 'personal data filing system' or simply 'filing system' it means any structured set of personal data which are accessible according to specific criteria, whether centralized or dispersed on a functional or geographical basis.[800] Also worth to note is to whom the Directive intends to protect. The initial scope is limited to the 'identified or identifiable natural person.'[801] However the Directive does not affect in any way legislation in member states which concern processing of data relating to legal/juristic

[791] Bygrave, p.32, note 503, supra.
[792] Directive 95/46/EC, Recital 25.
[793] There is, strictly speaking, a distinction between European Community law (EC law) and the European Union law(EU law). The former covers primarily matters pertaining to the internal market; it does not extend to police and judicial co-operation in criminal matters or to common foreign and security policy. The latter range of matters falls, however, under two other 'pillars' of the EU system; see Bygrave, p.34, note 503, supra.
[794] Directive 95/46/EC, Art 3(2).
[795] Ibid; see also Recital 12.
[796] See note 21,supra.
[797] Ibid, Paras 46 and 47 of the Judgement.
[798] Directive 95/46/EC, Recital 27.
[799] Ibid.
[800] Ibid, Art 2(c).
[801] Ibid, Art 2(a); see also detailed discussion in 2.2 of this thesis.

person.[802] The other point setting the limit of the application of the Directive is expressed in the form of obligations placed on 'controller,'[803] 'processor'[804] and 'third party'[805] in relation to 'processing'[806] of personal data.

d.) Data Protection Principles

The basic principles in the Directive parallel those laid down in the other international codes, especially the Council of Europe *Convention 108*.[807] Yet many of the principles in the Directive go considerably further than those in the other codes.[808] As such, discussion made over such codes is also relevant here although it is not reproduced. Generally, the Directive contains similar eight data protection principles. While such principles are not numbered in the Directive the present thesis numbers them only to facilitate their analyses and discussion.

The first principle requires that personal data must be processed fairly and lawfully.[809] For the processing of data to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection.[810] The 'lawfully' criterion relates to the authorization of the data processing either by law or data subject's consent.

The second principle states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[811] Further processing of data of historical, statistical or scientific purposes shall not be considered

---

802 Directive 95/46/EC, Recital 24; see also detailed discussion in 2.2 of this thesis.
803 'Controller' means a 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 the national or Community law, see Directive 95/46/EC, Art 2(d); see also detailed discussion in 2.2 of this thesis.
804 'Processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller, see Directive 95/46/EC, Art 2(e); see also detailed discussion in 2.2 of this thesis.
805 'Third party' means a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process data, see Directive 95/46/EC, Art 2(f).
806 'Processing of personal data or processing' means any operation or set of operations which is performed upon personal data, whether or not by automatic means such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, see Directive 95/46/EC, Art 2(b); see also detailed discussion in 2.2 of this thesis.
807 Bygrave, p.35, note 503, supra.
808 Ibid.
809 Directive 95/46/EC, Art 6(1),(a).
810 Ibid, Recital 38.
811 Ibid, Art 6(1),(b).

as incompatible provided that member states provide appropriate safeguards.[812] This principle is otherwise known as the purpose specification. It is important to mention that Art 7 lists the purposes for which the processing of personal data are considered to be legitimate. These criteria are listed in the alternative, if, (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 existence 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 purpose 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). The criteria laid down in Art 7 do not put very clear limits to the processing of personal data.[813] Yet the last two clauses are worth noting, because in Art 14, the data subject is given the right to object the processing of personal data under conditions (e) and (f).[814] The processing of personal data for commercial purposes is a central example of group (f).[815]

It is instructive at this juncture to introduce the most recent judgment of the European Court of Justice interpreting Art 7(f) of Directive 95/46/EC. The context of interpretation was prompted by the Spanish Tribunal Supremo which lodged a reference for a preliminary ruling to the ECJ on 28th September 2010 at the instance of *Asociación Nacional de Establecimientos Financieros de Crédito(ASNEF) v Administración del Estado.*[816] The gist of ASNEF's complaint was that Spanish law adds, to the condition relating to the legitimate interest in data processing without the data subject's consent, a condition, which does not exist in Directive 95/46, to the effect that data should appear in public sources.[817] In the Tribunal's view, that restriction constitutes a barrier to the free movement of personal data that is compatible with Directive 95/46 only if the interest of the fundamental rights and freedoms of the data subject so require.[818] Hence the only way to

[812] Ibid.
[813] Elgesem, p.285, note 427, supra.
[814] Ibid.
[815] Ibid.
[816] ECJ, C-468/10 and C-469/10).
[817] Ibid, Paragraph 17; see also generally Burgos, C and Pavón, B., 'Spanish Supreme Court provides Limited Relief for Data', Computer Law & Security Review, 2011, Vol.27, No. 1, pp.83-85.
[818] Ibid, Paragraph 20.

avoid a contradiction between Directive 95/46 and Spanish law is to hold that the free movement of personal data appearing in files other than those listed in Article 3(j) of Organic Law 15/1999[819] infringes the interest or the fundamental rights and freedoms of the data subject.[820] However being uncertain of its interpretation, the Tribunal Supremo referred two questions to the ECJ:-

1. Must Article 7(f) of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data be interpreted as precluding the application of national rules which, in the absence of the interested party's consent, and to which processing of his personal data that is necessary to pursue a legitimate interest of the controller or of third parties to whom the data will be disclosed, not only require fundamental rights and freedoms not to be prejudiced, but also require the data to appear in public sources?[821]

2. Are the conditions for conferring on it direct effect, set out in the case-law of the Court of Justice of the European Union, met by the above-mentioned Article 7(f)?[822]

In its judgment dated 24 November 2011, the ECJ answered both questions in the affirmative.[823] The paramount considerations given by the Court in its judgment were based on harmonization of the data protection laws across EU member states. With respect to the first question the ECJ drew its attention and reasoning on the object of the Directive. Essentially the Court upheld the second object in Art 1(2) which prevents member states from restricting or prohibiting the free

[819] Article 3(j) of Organic Law 15/1999 sets out 'public sources' in an exhaustive and restrictive list '...those files that can be consulted by any person, unhindered by a limiting provision or by any requirement other than, where relevant, payment of a fee. Public source are, exclusively, the electoral roll, telephone directories subject to the conditions laid down in the relevant regulations and lists of persons belonging to professional associations containing only data on the name, title, profession, activity, academic degree, address and an indication of membership of the association. Newspapers and official bulletins and the media are also public resources.' See also ECJ, C-468/10 and C-469/10), Paragraph 9.

[820] Note 818, supra.

[821] Ibid, Paragraph 22.

[822] Ibid.

[823] Ibid, Paragraphs 49 and 55: 'In light of those considerations, the answer to the first question is that Article 7(f) of Directive 95/46 must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also those data should appear in public resources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources...The answer to the second question is therefore that Article 7(f) of Directive 95/46 has direct effect.'

flow of personal data between member states by advancing reasons connected with protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy in the first object in Art 1(1). In its interpretation the ECJ cited recitals 7,8 and 10 which all of them carry the spirit of harmonization of member states' data protection laws. In finding affirmatively to the second question(which has also relevancy with the harmonization requirement) the ECJ relied on the settled case-law of the Court that whenever the provisions of a Directive appear, so far as their subject-matter is concerned, to be unconditional and sufficiently precise, they may be relied on before national courts by individuals against the state where the latter has failed to implement that Directive in domestic law by the end of the period prescribed or where it has failed to implement that Directive correctly.[824] The latter alternative applied to the Spanish data protection law in which case it imposed additional criterion which is incompatible with the Directive and has the effect of distorting harmonization of the EU data protection laws.[825]

The third principle is that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.[826] This principle is sometimes known as the minimality principle. It seeks to limit the amount of personal data under the control of data controllers to only what is necessary to achieve the purposes of such collection or further processing. The minimality principle is further reinforced by the requirement that personal data must be 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.[827] Accordingly, member states are obliged to lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[828]

The fourth principle requires that personal data must be 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.[829] This is otherwise known as the information quality

[824] See ECJ, C-203/10 Direktsia Obzhalvane i upravlenie na izpalnenieto Varna v Auto Nikolovi OOD [2011] ECR I-0000, paragraph 61; see also ECJ, C-468/10 and C-469/10), Paragraphs 51-55, note 816, supra.
[825] For the possible wide implications of the ECJ decision, see Alonso, C *et al*., 'ECJ Decision on Spain has Europe-wide Implications', Privacy Laws & Business International Report, 2011, No.114, pp.1,6-7.
[826] Directive 95/46/EC, Art 6(1),(c).
[827] Ibid, Art 6(1),(e).
[828] Ibid.
[829] Ibid, Art 6(1),(d).

principle. It has nexus to the minimality principle. Erasure and rectification are the primary remedies in case personal data are inaccurate or incomplete.

The fifth principle is sensitivity. This principle states that member states shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sexual life.[830] There are however exceptions to this general principle in which case sensitive personal data can still be processed where the data subject has given explicit consent to the processing of personal data;[831] or processing is necessary in carrying out the obligations and specific rights of the controller in the field of employment law;[832] or processing is necessary to protect vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;[833] or processing is carried out in the course of its legitimate activities with appropriate guarantees;[834] or the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.[835]

The sixth principle requires member states to provide that the data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[836] This principle is also known as information security principle. It further requires that where the data controller has engaged a processor to carry out data processing the former has to execute a contract or legal act binding the latter.[837] The contract or such legal act must stipulate that the processor shall act only on instructions from the controller and that the obligations set out in Art 17(1) as defined in the national legislation of the member state in which the processor is established shall also be incumbent to the processor.[838] For purposes of proof, the parts of the contract or legal act relating to data protection and the

[830] Ibid, Art 8(1).
[831] Ibid, Art 8(2),(a).
[832] Ibid, Art 8(2),(b).
[833] Ibid, Art 8(2),(c).
[834] Ibid, Art 8(2),(d).
[835] Ibid, Art 8(2),(a).
[836] Ibid, Art 17(1); see also Recital 46.
[837] Directive 95/46/EC, Art 17(3).
[838] Ibid.

requirements relating to measures referred in Art 17(1) need to be in writing or in another equivalent form.[839]

The seventh principle is transparency. This principle entails that the data controller and/or his representatives must identify themselves to the data subject without the latter's efforts to search or seek such identity.[840] Apart from disclosing their identity, the data controller and/or his representatives are obliged to notify the data subject the purposes of the processing for which the data are intended.[841] Also, they are obliged to provide further information such as the recipients or categories of recipients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the existence of the right of access to and the right to rectify the data concerning him-whether further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.[842] The transparency principle also imposes obligations on the data controller or his representatives to notify the supervisory authority established in accordance of a member state's national legislation before carrying out wholly or partly any automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.[843] The contents of the information required in the notification include identity of the data controller or his representatives, the purpose of the processing, description of the categories of the data subject and data relating to them, the recipient to whom the data might be disclosed, proposed transfers of data to third countries and a general description regarding preliminary assessment of the security of the processing.[844] Exemptions to the requirement of notification to supervisory authority are only allowed at a limited level.[845] The other obligation imposed on the data controller with respect to transparency is the registration requirement with the supervisory authority in a member state. All notifications by data controllers are required to be registered and be made subject of inspection by members of the public unless this poses security risks.[846]

Similar to automatic processing operations in relation to transparency principle are automated individual decisions. Article 15 of the Directive prohibits the data subject to be made subject of

[839] Ibid, Art 17(4).
[840] Ibid, Arts 10(a) and 11(a).
[841] Ibid, Arts10 (b) and 11(b).
[842] Ibid, Arts 10(c) and 11(c).
[843] Ibid, Art 18(1); see also Recital 54.
[844] Ibid, Art 19(1).
[845] Ibid, Art 18(2).
[846] Ibid, Art 21.

a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. However, this principle is subject to exceptions such as where there is a contract or law which safeguards the legitimate interests of the data subject.[847] The automated individual decision has been sometimes viewed as an independent data protection principle in the Directive.[848]

The eighth principle is data subject's participation. This right ensures that a data subject is placed in such a position as to influence the processing of information about him. Apart from that, the data subject's participation principle enables a data subject to protect his legitimate interests in the processing of his personal data. As such, the right entails that a data subject has access to the information about him held by the data controller or his representative;[849] that having gained such an access he is able to rectify or correct the information in case of any incompleteness or inaccuracies;[850] that he can object processing of any information about him (of course subject to the limitations of the national laws as allowed by the Directive)[851] and finally he has appropriate remedy in enforcing the mentioned rights.[852]

e.) Transborder Data Principles

As pointed out in 3.3.1.6 c, one of the objectives of the Directive is to ensure that there is a free flow of personal data between member states. Yet, circulation of personal information within the member states alone cannot foster international trade with non-member states (third countries). In realization of this limitation and possibly to resolve it, the Directive incorporates special rules of transfer of personal data to third countries in chapter IV comprising Arts 25 and 26.[853] The chief aim of these rules is to hinder data controllers from avoiding the requirements of data

[847] Ibid, Art15 (a) and (b).
[848] Bygrave, note 807, supra; for detailed discussion of automated individual decisions see generally Bygrave, Chapters 17 and 18, note 24, supra; Bygrave, L.A., 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', Computer Law & Security Report, 2001, Vol.17, No.1, pp.17-24; Schermer, B.W., 'The Limits of Privacy in Automated Profiling and Data Mining', Computer Law & Security Review, 2011, Vol. 27, No.1, pp. 45-52; Papakonstantinou, V., 'A Data Protection Approach to Matching Operations among Public Bodies', International Journal of Law and Information Technology, 2001, Vol.9, No.1, pp. 39-64.
[849] Directive 95/46/EC, Art 12(a).
[850] Ibid, Art 12(b).
[851] Ibid, Art 14.
[852] Ibid, Arts 22, 23 and 24.
[853] These two provisions must be read in conjunction with Recitals 56-60 in ascertaining their meaning.

protection laws by shifting their processing operations to countries with more lenient requirements (so-called 'data heavens').[854]

The main rule for TBDF in the Directive is provided in Art 25(1). It states that transfer of personal data to a third country which are undergoing processing or are intended for processing may take place only if the third country in question ensures an 'adequate level of protection'. In case the third country does not ensure 'adequate level of protection' the transfer of data to such country must be prohibited.[855] While the Directive does not define what is meant by 'adequate level of protection', it provides criteria for its assessment. Accordingly, Art 25(2) provides that the 'adequacy of the level of protection' afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations taking into account in particular the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. What clearly emerges from here is that Art 25 is not directed so much to the general provisions of the law in a third country, but the actual level of protection which will be accorded in a particular case.[856] This view is further cemented by the Article 29 Working Party who says, 'Article 25 envisages a case by case approach whereby assessment of adequacy is in relation to individual transfers or individual categories of transfers.'[857] Usually this assessment lies firstly with the data exporters (or transferors) and secondly with national data protection authorities in the EU/EEA.[858] However, the European Commission is empowered under Art 25(6) to make general determinations of 'adequacy' which are binding on EU (and EEA) member states.[859] In comparison with the data transferors and national supervisory authorities, the Commission is in a better position to assess

---

[854] Ellger, R., Der Datenschutz im grenzüberschreitende Datenverkehr: eine rechtsvergleichende und kollisions-rechtliche Untersuchung, Baden-Baden: Nomos, 1990, p87, cited in Bygrave, pp.79-80, note 24, supra.
[855] Directive 95/46/EC, Art 25(4), Recital 57.
[856] Aldhouse, F., 'The Transfer of Personal Data to Third Countries under EU Directive 95/46/EC', International Review of Law Computers & Technology, 1999, Vol.13, No.1, pp.75-79, at p.76.
[857] Article 29 Data Protection Working Party, 'Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy', XV D/5020/97/ EN, WP 4, (adopted on 26th June 1997), p.1.
[858] Bygrave, p.81, note 24, supra; see also Article 29 Data Protection Working Party, p.2, note 857, supra.
[859] Bygrave, note 858, supra; note also that the Commission does not make such decisions on its own but with input from (i) the Data Protection Working Party(which may deliver a non-binding opinion on the proposed decision(Art. 30(1)(a) & (b); the Article 31 Committee (whose approval of the proposed decision is necessary and which may refer the matter to the Council for final determination (Art. 31(2)); and (iii) the European Parliament(which is able to check whether the Commission has properly used its powers), see Bygrave(footnote 317), note 858, supra; see also European Commission., 'Commission decisions on the adequacy of the protection of personal data in third countries', http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm last visited 7/1/2012.

the adequacy of data protection.[860] Such a holistic approach is cost efficient.[861] Moreover, it relieves member states as they do not have to assess the same cases, and differences between national assessments can be avoided.[862] Similarly, this approach increases certainty and predictability for data transferors.[863] As a result, the overall effect of the Commission's positive determinations is to allow free flow of personal data from the 27 EU member states and three EEA member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.[864] Currently the European Commission has recognized Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, Australia, Faeroe Islands, Andorra, Israel, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.[865] Also important to bear in mind is that in all cases where a member state or the Commission considers that a third country does not ensure an adequate level of protection of personal data within the meaning of Art 25(2), such information

---

860 Kong, L., 'Data Protection and Transborder Data Flow in the European and Global Context', The European Journal of International Law (EJIL), 2010, Vol. 21, No.2, pp.441-456, at p. 445.
861 Ibid.
862 Ibid.
863 Ibid.
864 European Commission, note 859, supra.
865 COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, 2000/518/EC of 26 July 2000 - O. J. L 215/1, 25/8/2000; COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, C(2000) 2441 of 26 July 2000- O. J. L 215/7, 25/8/2000; COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, C(2001) 4539 of 20 December 2001- O.J. L 2/13, 4/1/2002; COUNCIL DECISION on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data, 2006/230/EC of 18 June 2005-O.J.L 82/14, 21/3/2006; COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, C(2003) 1731 of 30 June 2003 – O.J.L 168, 5/7/2003; COMMISSION DECISION on the adequate protection of personal data in Guernsey, C(2003) 4309 of 21 November 2003 – O.J.L 308, 25/11/2003; COMMISSION DECISION on the adequate protection of personal data in the Isle of Man, C(2004) 1556 of 28 April 2004-O.J. L 151/48, 30/4/2004; COMMISSION DECISION on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, C(2004) 1914 of 14 May 2004, COMMISSION DECISION on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, C(2005) 3248 of 6 September 2005; COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, C(2008) 1746 of 8 May 2008 - OJ L 138/21, 28/5/2008; COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service, C 2008/651/CFSP/JHA of 30 June 2008, O.J.L213/47, 08/08/2008; COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data, C(2010) 1130) of 5 March 2010 – O.J.L58/17, 9/3/2010; COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra, C(2010) 7084 of 19 October 2010 – O.J. L 277/27, 21/10/2010; and COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, C(2011) 332 of 31 January 2011- O.J.L 27/39, 1/2/2011.

is required to be shared across member states. Yet, it is doubtful if in the former case the notification may have a binding effect on the other member states.

The second set of rules of TBDF relates to the derogations from the above main rule. These derogations are provided in Art 26. They apply where a third country does not provide 'adequate level of protection' to transfer of personal data. Art 26(1) lays down six criteria in the alternative to be fulfilled before a transfer of personal data to such third country can be permitted (a) that the data subject has given consent unambiguously to the proposed transfer; or (b) the transfer is necessary to perform certain contracts between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract with a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary to protect the vital interests of the data subject;[866] or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

Art 26(2) provides another possibility of derogation. In this case, transfer of personal data may be authorized by a member state where the data controller adduces 'adequate safeguards' with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses. The 'adequate safeguards' referred in this provision are not in any way less than the 'adequate protection' standard which consists of a series of basic data protection principles together with certain conditions necessary to ensure their effectiveness.[867] Also to ensure that these arrangements do not weaken the level of protection of personal data, a member state which has so authorized transfer of personal data in accordance with Art 26(2) is required to notify the other member states and Commission.[868] If upon such notification a member state or the Commission objects the assessment on justified grounds the latter will take

[866] The expression 'vital interest' of the data subject has a restrictive meaning to mean 'which is essential for the data subject's life', see Directive 95/46/EC, Recital 31.
[867] Article 29 Data Protection Working Party, 'Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive', DG XV D/5025/98/WP 12, (adopted on 24th July 1998), p.17. See also 3.3.1.6.e (i), (ii) and (iii) of this thesis for discussion of the data protection principles and mechanisms of their enforcement as envisaged by the Article 29 Working Party.
[868] Directive 95/46/EC, Art 26(3).

appropriate measures in which case member states shall comply with it.[869] Finally, the Commission may decide that certain standard contractual clauses offer sufficient safeguards in terms of Art 26(2).

The implementation of Arts 25 and 26 have generated intense debates and commentaries. Yet, up to recently various interpretations and commentaries of these provisions have failed to offer proper scope with certainty. This has significantly reduced the practical utility and complicated the enforcement of the Directive. For example, the Article 29 Working Party and Commission have issued various documents attempting to interpret and how to implement Arts 25 and 26, yet these have not resolved the difficulties in actual practice. Two main sets of such documents may be identified as general and specific guidance. The former sort of documents include Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy,[870] Working Document on Judging Industry Self-Regulation: when does it make a meaningful contribution to the level of data protection in a third country?,[871] Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive[872] and Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.[873] On the other hand, specific documents adopted by the Article 29 Working Party and Commission include: Working Document: Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries,[874] Opinion 1/2001 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Article 26(4) of Directive 95/46,[875] Opinion 7/2001 on the Draft Commission Decision(Version 31 August 2001) on Standard Contractual Clauses for the Transfer of Personal to Data Processors established in Third Countries under Article 26(4) of Directive 95/46,[876] Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors established in Third Countries, under Directive 95/46/EC,[877] Working Document on Transfer of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive on Binding Corporate Rules for

[869] Ibid.
[870] Article 29 Data Protection Working Party, note 857, supra.
[871] DG XV D/5057/97/ WP 7, (adopted on 14th January 1998).
[872] Article 29 Data Protection Working Party, note 867, supra. .
[873] 2093/05/EN, WP 114, (adopted on 25th November 2005).
[874] DG XV D/5005/98, WP 9, (adopted on 22nd April 1998).
[875] 5006/02/EN, WP 38, (adopted on 26th January 2001).
[876] 5061/01/EN, WP 47, (adopted on 13th September 2001).
[877] Commission Decision, (EC) 2002/16/EC, O.J.L 6, 27 December 2001, pp.52-62.

International Data Transfer,[878] Opinion 8/2003 on the Draft Standard Contractual Clauses by a Group of Business Associations ('the Alternative Model Contract'),[879] Recommendation 1/2007 on the Standard Application of Binding Corporate Rules for the Transfer of Personal Data,[880] Working Document setting up a table with the elements and principles to be found in the Binding Corporate Rules,[881] Working Document setting up a Framework for the Structure of Binding Corporate Rules,[882] Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules,[883] Opinion 3/2009 on Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors established in Third Countries, under Directive 95/46/EC (Data Controller to Data Processor),[884] Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors established in Third Parties under Directive 95/46/EC of the European Parliament and of the Council,[885] FQAs in order to address some issue raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors established in Third Countries under Directive 95/46/EC,[886] Opinion 7/2010 on European Commission's Communication on the Global Approach to Transfers of Passenger Name Record(PNR) Data to Third Countries,[887] and Opinion 10/2011 on the Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Records Data for Prevention, Detention, Investigation and prosecution of Terrorist Offences and Serious Crimes.[888]

Apart from the above list of specific documents, there is a long list of specific documents on TBDF between the European Union and the United States of America. The latter are considered in 3.3.2 of this thesis.

Worthwhile to note is that more than any other document in the above list *Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection*

878 11639/02/EN, WP 74, (adopted on 24th October 2002).
879 11754/03/EN, WP 84, (adopted on 3rd June 2003).
880 WP 133, (adopted on 1st January 2007).
881 1271-00-00/08/EN, WP 153, (adopted on 24th June 2008).
882 1271-00-01/08/EN, WP 154, (adopted on 24th June 2008).
883 1271-04-02/08/EN, WP 155 rev.04, (adopted on 24th June 2008, last revised on 8th April 2009).
884 00566/09/EN, WP 161, (adopted on 5th March 2009).
885 Commission Decision, (EC) 2010/87/EU, O.J.L 39, 5 February 2010, pp.5-9. For a detailed discussion of the Commission's Decision, see Wojtan, B., 'The new EU Model Clauses: One Step Forward, Two Steps Back?', International Data Privacy Law, 2011, Vol.1, No.1, pp. 76-80.
886 00070/2010/EN, WP 176, (adopted on 12th July 2010).
887 622/10/EN, WP 178, (adopted on 12th November 2011).
888 00664/11/EN, WP 181, (adopted on 5th April 2011).

Directive[889] or simply WP 12 contains detailed methodological criteria of assessment of 'adequacy' requirement. It is therefore interesting to examine such methodology as it cuts across all other documents. Also, the examination alerts non-EU countries which have not so far adopted data protection legislation or which have adopted such legislation but have not yet been accredited by EU as having adequate data protection regulations and practices to appreciate what is expected from them by EU if they wish to continue to exchange personal data with the latter.

WP 12 sets out two levels of assessment of 'adequate level of data protection' with regard to transborder flow of personal data to third countries. The first level of assessment relates to 'content' principles while the second 'procedural/enforcement'. In principle, the former are modified version of the data protection principles contained in the of Directive 95/46/EC (see 3.3.1.6 d) while the latter mirror the enforcement mechanisms envisaged to a large extent under chapters VI of the Directive(see 3.3.1.6 f).

i. Substantive Content Principles

- **The Purpose Limitation Principle**

Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 12 of the Directive.

- **The Data Quality and Proportionality Principle**

Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

- **The Transparency Principle**

Individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is

[889] See notes 867 and 872, supra.

necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the Directive.

- **The Security Principle**

Technical and organizational security measures should be taken by the data controller that are appropriate to the risks presented by processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

- **Rights of Access, Rectification and Opposition**

The data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to those rights should be in line with Article 13 of the Directive.

- **Restrictions on Onward Transfers**

Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the Directive.

ii. Additional Principles to be applied to Specific Types of Processing

- **Sensitive Data**

Where 'sensitive' categories of data are involved (those listed Article 8 of the Directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

- **Direct Marketing**

Where data are transferred for purposes of direct marketing, the data subject should be able to 'opt out' from having his/her data used for such purposes at any stage.

- **Automated Individual Decision**

Where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the Directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

iii. Procedural/Enforcement Mechanisms

In Europe the enforcement mechanism of data protection laws rest with the national supervisory authorities (see 3.3.1.6 f). However since in most non-EU member states the existence of comprehensive data protection legislation and concomitantly the supervisory authorities are lacking, the WP 12 adopts an evaluation method that is flexible. This entails first, identification of the underlying objectives of a data protection procedural system, and second judgment of different judicial and non-judicial procedural mechanisms used in third countries. Accordingly WP 12 identifies three main objectives of a data protection system:-

- **Delivery of a good level of compliance with the rules**

A good system is generally characterized by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

- **Provision of support and help to individual data subjects in the exercise of their rights**

The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

- **Provision of appropriate redress to the injured party where rules are not complied with**

This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

In winding up this part, it is imperative to highlight key points relating to TBDF under Arts 25 and 26 of the Directive 95/46/EC. First, more than any other rules of TBDF contained in the international codes of data protection, Art 25 and 26 have exercised strong political pressure on non-EU member states to adopt comprehensive data protection legislation in the EU-style.[890] Second, although in principle an 'adequate level of data protection' can be attained through self-regulation it is hardly possible for a third country to be generally considered as satisfying the required level of adequacy merely on the basis of self-regulations. This is not surprising because self-regulations are restrictive in their application. They only cover and bind particular sectors or members of specific professions as such an individual falling outside cannot enforce his or her rights and obtain appropriate remedies. The other limitation facing self-regulations is the lack of sound enforcement mechanisms.[891] Third, given that under Directive 95/46/EC there are two different types of assessment of 'adequate level of data protection': the general assessment by the European Commission which may cover either the entire third country or specific sectors within such country and specific assessments relating to each specific transfer determined by controllers or national supervisory authorities, the likelihood of divergences of assessments are bound to

[890] All of these provisions give an impression that the EU, in effect, is legislating for the world; Bygrave, p. 334, note 25, supra.

[891] Blume, P., 'Transborder Data Flow: Is there a solution in sight?', International Journal of Law and International Technology, 2000, pp.65-86, at p.70; see also The Working Group-Latin America Data Protection Network, 'Self-Regulation and Personal Data Protection', Conference at Santa Cruz De La Sierra-Bolivia, 3-5 May 2006, pp.1-13, http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Autorregulacion_Ingles.pdf , last visited 9/01/2012, where self-regulation was clearly held to be ineffective means of achieving adequate data protection; see also Gellman, R and Dixon, P., 'The History of failed Self-Regulation in the United States', Privacy Laws & Business International Report, 2011, No.114, pp.10-12.

occur. The likelihood is further made a reality with the different ways EU member states have transposed the Directive which allows them some margins of maneuvering the general principles laid down there. Fourth, although the Article 29 Working Party has attempted to lay down legally non-binding rules for assessment of 'adequate level of data protection' in the third countries particularly those found in WP 7 and WP 12, in practice, it has taken into account extraneous latent considerations not envisaged by the Directive itself. For example, the Article 29 Working Party commissioners have considered and hence taken on board political considerations in the assessment. In their view 'some third countries might come to see the absence of a finding that they provided adequacy protection as politically provocative or at least discriminatory, in that the absence of a finding is as likely to be the result of their case not having been examined as of a judgment on their data protection system.'[892] Performing the adequate assessment on these fears has rendered 'political considerations an obstacle for a sound evaluation, as not placing a country on the white list is similar to blacklisting it'.[893] Yet, in mitigating the chances of occurrence of diplomatic and political tensions with third countries, the EU has in most cases awaited third countries to initiate the process of accreditation.[894] In such cases even if at the first instance the Commission finds problems with the data protection regulations and practices in a third country, it normally engages such countries and facilitates improvement of their regulations and practices until a required level is reached.[895] In such approach the Article 29 Working Party, the technical group of EU which advises the Commission, more often adopts its official opinion on the level of adequacy after the third countries have addressed a number of areas of concerns. Because of this, most of its adopted opinions have had favorable outcome on third countries (except the US Safe Harbor Agreement and the Passenger Name Records which present a different story, see

[892] Article 29 Data Protection Working Party, p. 27, note 867, supra; see also Kong, note 860, supra.
[893] Blume, note 891, supra.
[894] See e.g., Ringou, N., 'Data Protection: European Adequacy Procedure', presentation made in 'Twinning Project IS/2007/ENPAP/JH/01: Strengthening Data Protection in Israel' 30 September 2009, Israel, (23 slides, at slide no.17),http://www.justice.gov.il/NR/rdonlyres/A31C13F2-3554-4086-929C-2CFF6D31462C/21169/DataProtectionIsrael.pdf last visited 11/01/2012.
[895] Ibid, slide no.18; see e.g., Article 29 Data Protection Working Party, 'Opinion 6/2009 on the Level of Protection of Personal Data in Israel', 02316/09/EN, WP 165, (adopted on 1st December 2009), pp.17-18 where even after the Article 29 Working Party had made a finding that Israel's system of data protection law meets the adequate level of data protection under the Directive, the former proceeded to encourage the latter to specifically improve its system in future legislative development in the following aspects: the extension of application of the Israeli legislation to manual databases; the express inclusion of the proportionality principle in relation to the totality of personal data processing carried out by the private sector, and incorporation of interpretation of the exemptions in international data transfers online envisaged in Article 26(1) of the Directive. This was also the case for Argentina where the Article 29 Working Party says, 'the Working Party encourages the Argentinean authorities to take the necessary steps to overcome some remaining weaknesses in the present legal instruments, as identified in this opinion and requests the Commission to continue the dialogue with the Argentinean Government with that purpose. In particular the Working Party urges the Argentinean Authorities to ensure the effective enforcement of the legislation at provisional level by means of the creation of the necessary independent control authorities where they do not exist yet and, in the mean-time, to look for appropriate temporary solutions in accordance with the Argentinean Constitutional order.

3.3.2).[896] Yet, where the Article 29 Working Party had a negative opinion as to the 'adequate level of data protection' in a third country it used a 'neutral' language in its opinion to avoid passing a direct 'verdict' but only through expressing its dissatisfaction by drawing the attention of the Commission to take into account key areas of concerns when making its decision. This was the case, for example, with the determination of 'adequacy' of the Canadian Personal Information and Electronic Documents Act 2000.[897] However in those cases where express negative opinion is issued this has never been publicized. In this connection Professor Graham Greenleaf argues:-

> 'There could be significantly more adequacy findings outside Europe if the EU was more pro-active and more transparent about its processes. Where the EU has made positive adequacy decision it has publicized the reasons, but where it has considered "applications" from other countries but concluded that their protections were not yet adequate, it has not generally publicized the reasons for these negative conclusions. There has therefore been much less information available about what does and what does not constitute "adequacy" than is desirable.'[898]

The approach is different in some occasions where external consultants had been hired by the Commission to undertake analysis of the adequacy of data protection in a third country. Here a

---

[896] The list of the Article 29 Working Party opinion since the adoption of the Directive up to January 2012(excluding those on USA) include: 'Opinion 5/99 on the Level of Protection of Personal Data in Switzerland', 5054/99, WP 22, (adopted on 7th June 1999); 'Opinion 6/99 on the Level of Personal Data Protection in Hungary', 5070/EN/99, WP 24, (adopted on 7th September 1999); 'Opinion 3/2001 on the Adequacy Level of the Canadian Personal Information and Electronic Documents Act', 5109/00/EN, WP 39, (adopted on 26th January 2001); 'Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment(Private Sector) Act 2000', note 164, supra; 'Opinion 4/2002 on the Level of Protection of Personal Data in Argentina', 11081/02/EN, WP 63, (adopted on 3rd October 2002); 'Opinion 5/2003 on the Level of Protection of Personal Data in Guernsey', 10595/03/EN, WP 79, (adopted on 13th October 2003); 'Opinion 6/2003 on the Level of Protection of Personal Data in the Isle of Man', 11580/03/EN, WP 82, (adopted on 21st November 2003); 'Opinion 1/2004 on the Level of Protection of Personal Data ensured in Australia for the Transmission of Passenger Name Record Data from Airlines', 10031/03/EN, WP 85, (adopted on 16th January 2004); 'Opinion 3/2004 on the Level of Protection ensured in Canada for the Transmission of Passenger Name Records and Advance Passenger Information from Airlines', 10037/04/EN, WP 88, (adopted on 11th February 2004); 'Opinion 1/2005 on the Level of Protection ensured in Canada for the Transmission of Passenger Name Record and Advance Passenger Information from Airlines', 1112/05/EN, WP 103, (adopted on 19th January 2005); 'Opinion 8/2007 on the Level of Protection of Personal Data in Jersey', 02072/07EN, WP 141, (adopted on 9th October 2007); 'Opinion 9/2007 on the Level of Protection of Personal Data in the Faroe Islands', 02107/07/EN, WP 142, (adopted on 9th October 2007); 'Opinion 6/2009 on the Level of Protection of Personal Data in Israel', note 893, supra; 'Opinion 7/2007 on the Level of Protection of Personal Data in the Principality of Andorra', 02317/09/EN, WP 166, (adopted on 1st December 2009); 'Opinion 6/2010 on the Level of Protection of Personal Data in the Eastern Republic of Uruguay', 0475/10/EN, WP 177, (adopted on 12th October 2010); and 'Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand', note 311, supra.

[897] Article 29 Data Protection Working Party, p.7, note 896, supra.

[898] Greenleaf, G., 'Do not dismiss "Adequacy": European Standards entrenched', Privacy Laws & Business International Report, 2011, No.114, pp.16-18, at pp.16-17.

more direct language has been used in those instances of negative findings. For instance, the conclusive view of the consultants (Research Centre in IT and Law, University of Namur, Belgium) in case of Tunisia's analysis of adequacy level of data protection is that 'the Tunisian regime regarding the protection of personal data is to be considered *inadequate*, at the present time, and on the basis of our comprehension of the Act in force.'[899] Perhaps because of this, in those cases reports on adequacy have either been treated confidential allegedly on account of contractual confidentiality clauses between the consultant and the Commission[900] but in reality to prevent the so called 'political provocation' which the Article 29 Working Party has openly admitted in its guidelines for assessing the level of adequacy of data protection in third countries

[899] CRID (*Centre de Recherches Informatique et Droit*), University of Namur (Belgium)., 'Analysis of the Adequacy of Protection of Personal Data provided in Tunisia-Final Report', 2010, at p. 123, http://alexandrie.droit.fundp.ac.be/GEIDEFile/6544.pdf?Archive=192619191089&File=6544_pdf, last visited 10/01/2012. It is interesting to note that in similar assessment of adequacy for India, CRID avoided to explicitly say that India does not provide adequate level of data protection though the impression left in the conclusion is meant to be so; see CRID, University of Namur (Belgium)., 'First Analysis of the Personal Data Protection in India-Final Report', 2005, pp.70-71, http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf last visited 15/01/2012. For a detailed discussion about Indian conception of privacy and possibly why it is slow in enacting data protection similar to EU see e.g., Basu, S., 'Policy-Making, Technology and Privacy in India', The Indian Journal of Law and Technology, 2010, Vol.6, pp.65-88.

[900] The confirmation of this claim was made to the researcher via email on 10/01/2012 by Prof. Cécile de Terwangne when the former requested from the latter supply of CRID., 'Analysis of the adequacy of protection of personal data provided in Mauritius: draft final report, 2010', prepared by Claire Gayrel, Florence de Villenfagne, Cécile de Terwangne who declined to make such a supply but advised the researcher to make a direct request from the European Commission. The researcher also received similar response from the Commissioner of Data Protection in Mauritius by email sent on 10/01/2012 when he requested the same report. However, the Commissioner promised to send the second report to the researcher a month later suggesting that report may have a favourable assessment from EU authorities. The confidentiality syndrome has featured in other reports of the CRID expressly marked as confidential: CRID., 'First analysis on the personal data protection law in Albania to determinate whether a second step has to be undertaken : final report (confidentiel), 2006', prepared by Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Virginie Fossoul, Yves Poullet, Artur Asslani, Gianluca Carlesso; CRID., 'First analysis of the personal data protection law in Bosnia and Herzegovina in order to determinate whether a second step has to be undertaken (confidentiel), 2006', prepared by Cécile de Terwangne, , Florence de Villenfagne, Franck DumortieR, Virginie Fossoul, Yves, Poullet; CRID., 'First analysis of the personal data protection law in Fyrom in order to determinate whether a second step has to be undertaken (confidentiel), 2006', prepared by Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Virginie Fossoul, Yves Poullet, Neda Korunovska; CRID., 'Analysis of the adequacy of protection of personal data in the Faeroe Islands (confidentiel), 2006', prepared by Permille Wegener Jessen, Evelyne Beatrix Cleff, Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Yves Poullet; CRID., 'First analysis of the personal data protection law in Israel in order to determinate whether a second step has to be undertaken (confidentiel), 2006', prepared by Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Virginie Fossoul, Yves Poullet, Michael Dan Birhack; CRID., 'First analysis of the personal data protection law in Japan in order to determinate whether a second step has to be undertaken (confidentiel), 2006', prepared by Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Virginie Fossoul, Yves Poullet, Masao Horibe; CRID., 'First analysis of the personal data protection law in Kosovo in order to determinate whether a second step has to be undertaken : final report (confidentiel), 2006', prepared by Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Virginie Fossoul, Yves Poullet; CRID., 'First analysis of the personal datat protection in Montenegro to determinate whether a second step has to be undertaken : final report (confidentiel), 2006', prepared by Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Virginie Fossoul, Yves Poullet, Sasa Gajin; and CRID., 'First analysis of the personal datat protection in Serbia to determinate whether a second step has to be undertaken : final report (confidentiel), 2006', prepared by Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Virginie Fossoul, Yves Poullet, Sasa Gajin; http://alexandrie.droit.fundp.ac.be/Record.htm?Record=191290861579194726 89&idlist=6 last visited 12/01/2012. It is important to note that while the list of these reports is available at CRID website, their contents are not accessible.

as a potential risk to diplomatic relations.[901] Yet, only rarely such reports have been made public.[902] The other extraneous criterion considered by the Article 29 Working Party in its opinion is the economic importance of a third country to Europe and concomitantly the amount of data of Europeans likely to be transferred there. This can well be demonstrated by the recent clearance of New Zealand by the Article 29 Working Party as providing adequate level of data protection despite several weaknesses in the New Zealand's data protection regime. It is evident that the clearance was prompted by 'the New Zealand's relative geographical isolation; the limited EU-sourced data likely to be transferred to New Zealand (which minimizes the problem of onward transfers); and the reciprocal lack of direct marketing into the EU that could be expected from NZ'.[903] It can thus be generally concluded 'that the standard of adequacy is in inverse proportion to proximity, provided that "proximity" is considered to include the economic and social, not only the geographical'.[904] Also significant, the Article 29 Working Party has taken into consideration the interests of EU citizens at the expense of those in the third country when assessing the adequacy of the data protection system. Accordingly 'it is the effect of a third party's laws on EU citizens that counts toward adequacy, not the effect on the country's own citizens'.[905] Finally, the EU has double standard in terms of the criteria for transfer of personal data: the 'equivalency' criterion applies to EU member states while the 'adequacy' is invoked against third countries. Arguably, this is likely to result into unnecessary disparities in implementation of the Directive.

Linked to TBDF are conflicts of laws issues. As noted, none of the previous international codes regulating protection of personal data (notably the *OECD Guidelines*, *Convention 108* and *UN Guidelines*) contains applicable law rules (also known as conflict of laws, choice of law, interlegal issues or private law issues). In contrast, Art 4 of Directive 95/46/EC contains the first and the only set of an international data protection instrument to deal specifically with the determination of applicable law.[906] Art 4 reads:-

---

[901] Article 29 Data Protection Working Party, note 892, supra.
[902] See e.g., CRID, note 899.
[903] Greenleaf, G and Bygrave, L.A., 'Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection', Privacy Laws & Business International Report, 2011, No.111, pp.8-9, at p. 9.
[904] Ibid.
[905] Ibid.
[906] Bing, J., 'Data Protection, Jurisdiction and the Choice of Law', Privacy Law & Policy Reporter, 1999, Vol. 6, No. 6, pp. 92-98. This article is no longer downloadable in pdf format from http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/PLPR/1999/65.html?stem=0&synonyms=0&query=Bing#disp1 where it was first published hence difficult to cite the specific page number referred. However the same paper is available in html at https://www.pco.org.hk/textonly/english/infocentre/files/bing-paper.doc last visited 13/01/2012, pp. 1-11, at p. 7; see also Bygrave, note 500, supra.

'Article 4: National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
   (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
   (b) the controller is not established on the member State's territory, but in place where its national law applies by virtue of international public law;
   (c) the controller is not established on the Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of the Member State, without prejudice to legal actions which could be initiated against the controller himself.'

The above provisions of Art 4 have generated quite substantial but conflicting interpretations from commentators, national supervisory authorities in EU member states and the Article 29 Working Party. As can be noted, Art 4 contains two sets of rules of applicable law: those relating to EU member states and those relating to third countries. Both sets have some interactions at some points; hence any discussion of Art 4 must not be made in isolation of the other. However, before analyzing these rules it is important to underscore the rationale behind their incorporation in the Directive.

The rationale behind Art 4 can generally be traced from the aims of the Directive: to ensure protection of fundamental rights and freedoms of the individuals as well as free flow of

information across the EU member states. Based on these objectives several principles were incorporated in the Directive. One category of these principles relate to enforcement-i.e. institutions of enforcement such as supervisory authorities, courts and other administrative bodies; remedies and sanctions. In practice, enforcement is impossible if there is uncertainty as to which law individuals are subject to. In that regard, Art 4 was adopted to determine which law applies when and to whom. Also, the adoption of Art 4 was to ensure there is harmonization in application of the law across EU reflecting the overall purpose of Directive 95/46/EC. This has been explained in the *travaux préparatoires* in the following words, 'that the same processing operation might be governed by the laws of more than one country'[907] hence disparities in the level of protection. The other rationale explained in the *travaux préparatoires* of the Directive is to prevent data controllers in EU to circumvent the EU data protection regime by relocating their processing activities to third countries-the so called 'data havens'. As a result of this circumvention, the data subject might find himself outside any system of protection.[908] It can be argued, at least contrary to Lokke Moerel's view,[909] that although the final version of Directive 95/46/EC abandoned the 'country of origin principle' to which the Explanatory Memorandum to the Amended Proposal of the Original[910] version was meant for, the former (i.e. the final version of the Directive) sought to continue to retain the spirit of the objective of Art 4 in the Amended Proposal. In other words, the final version of the Directive only changed the method or approach of applicable law from the 'country of origin principle' to 'territoriality principle'. Confirmation of this view can be derived from two sources. First is the Explanatory Memorandum to the Original version of Directive 95/46/EC itself which Moerel overlooked to refer and focused on the Explanatory Memorandum of the Amended Proposal. According to the former, the objectives of Art 4 as incorporated in the Original version of the Directive were explained in the following words:-

---

907 Commission of the European Communities., 'Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data', COM (92) 422 final, 15 October 1992, p.13; see also Bygrave, p.253, note 50, supra.

908 Ibid.

909 'Some commentators (referring to Lee A. Bygrave in his article-Determining Applicable Law Pursuant to European Data Protection Legislation-see note 906, supra and Jon Bing in his article-Data Protection, Jurisdiction and the Choice of Law-see note 906, supra) interpret Article 4(1)(a) as leading to the applicability of the law of the Member State where the controller is established. Some quote in support of this interpretation the Explanatory Memorandum of the Commission (referring to Bygrave and Bing), where the Commission gives the second rationale for the applicability rule of Article 4(1)(a) "to avoid that one and the same data processing would be governed by the law of more than one country". As noted above, this Memorandum was published in respect of the Amended Proposal, therefore at the time the country of the origin principle was still contained in the proposed Directive, a point these commentators have overlooked'-Moerel, L., 'Back to Basics: When does EU Data Protection Law apply?', International Data Privacy Law, 2011, Vol.1, No.2, pp. 92-110, at p.103.

910 See, note 907, supra.

> 'This article specifies the connecting factors which determine the application in each Member State of the Directive's provisions. The choice of factors in paragraph 1 is motivated by the desire to avoid a situation in which the data subject is completely unprotected owing, mainly, to the law being circumvented. The factual criterion of the place in which the file is located has therefore been adopted. In this connection, each part of a file which is geographically dispersed or divided among several Member States must be treated as a separate file. The desire to protect the data subject in the event of relocation is at the root of a provision which requires a user consulting a file located in a third country from a terminal located in a Member State to comply with the Directive's provisions…This Article is also designed to avoid any overlapping of applicable laws.'[911]

The above paragraph was replicated in the Explanatory Memorandum of the Amended Proposal with only a change of connecting factor from 'location of the file' to 'place of establishment of the controller' but with the retention of the 'country of origin principle' and the objective behind it. The second source of confirmation of the continuity or rather retention of the objective behind Art 4 is recitals 19 and 20 of the preamble to the final version of the Directive. Recital 19 reflects the prevention of any possible circumvention of the national rules. It reads:-

> 'Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member states, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities'

Recital 20 relates to the objective of ensuring respect for rights and obligations provided in the Directive. It provides:-

[911] Commission of the European Communities., 'Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data', COM (1990), final-SYN 287, 13 September 1990, pp. 21-22.

> 'Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice.'

Moreover, cases I-V cited and discussed by Moerel (as Opinion 2-i.e opposing interpretation to what is envisaged under Art 4)[912] seem not to be justified on objectives of Art 4 as explained in the Explanatory Memorandum to the Amended Proposal of the Directive although some of the views are in line with Bygrave and Bing. This weakens any proposition that the misinterpretation of Art 4 of the Directive is linked to reckoning the objective of Art 4 on the Explanatory Memorandum to the Amended Directive.

In substance, the Directive's applicable law is wholly based on the 'territoriality' principle. This principle applies regardless of whether processing of personal data has taken place within EU member states or in relation to international processing (i.e. involving third countries). Art 4 lays down two connecting factors to the 'territoriality principle'. The first, and which commentators have widely cited as main default rule, is 'the context of the activities of an establishment of the controller on the territory of the Member State' in Art 4(1)(a). Accordingly it is not 'the place of establishment'[913] but the 'the place where the activities of an establishment of the controller' has taken place on the territory of a member state which is considered. The difference between the two criteria is that while the former relates such activities to the seat or place of incorporation of a controller (i.e. referring to the application of the 'country of origin principle') the latter relates only to the place where the activities of the controller has direct bearing without physically being established there. Lokke Moerel distinguishes these two criteria by relating the former to 'being established' and the latter 'having an establishment'.[914] According to this author, the concept 'being established' refers to the primary establishment of the controller and serves the country of

[912] Moerel, pp.103-106, note 909, supra.
[913] For contrary view see e.g., Bygrave, note 907 who argues, ' It can be seen that, under Art 4, the principle criterion for determining applicable law is the data controller's place of establishment, largelrly irrespective of where the data processing occurs.' Similar view is held by Bing, pp.6-7, note 906, supra. Yet in a subsequent article, Bing, J., 'The identification of applicable law and liability with regard to the use of protected material in the digital context', ECLIP Research Report, 2000, pp.236-258, at 248, the author(Jon Bing) appears to shift from his earlier position as to the applicability of Art 4 where he argues, 'This does not, perhaps, make it quite clear what an "establishment" implies but it would clearly include subsidiaries, branch offices, and perhaps also agents or similar representation. In any case, the criterion is based on the activity of the controller.'
[914] Moerel, p. 94, note 909, supra.

origin principle while 'having an establishment' which is the basis for the applicability rule of the Directive, includes the primary establishment but especially refers to secondary establishments like subsidiaries, branches, and agencies.[915] In this context therefore, the applicable law is the law of the country in which the controller's data processing activities relate to and not the law of the country where it has its primary establishment. The Directive seems to declare a national data protection law already applicable if the data processing takes place in the context of the activities of an establishment of a controller that is located on its territory.[916] There is yet another criterion under Art 4(1)(a) where the same controller is established on the territory of several member states. In such a situation each of the establishments of a controller has to comply to the national law applicable in respective territories. Accordingly, the laws of more member states may apply to a processing of personal data (i.e. commutation of applicable laws).[917]

Where the controller is not established on the territory of the member state two rules apply but not cumulatively. The first, which is less problematic, is Art 4(1)(b). This is the instance where according to the rules of public international law, the national law of a state applies. This rule extends to the field of application of public law.[918] Suffice to say that there has been little discussion on this provision presumably because it has not caused much difficulty to apply. Much more complex application and accordingly commentaries have arisen with respect to Art 4(1)(c). It has sometimes tempted commentators to regard this as the second main default rule of applicable law under Art 4 leaving out entirely Art 4(1)(b). The connecting factor for making Art 4(1)(c) applicable is 'use of equipment' located on the territory of a member state. 'Transit' through such 'equipment' is excluded from 'use of equipment'. The latter expression is not defined in the Directive. Yet, when one reads Art 4(1)(c) of the Directive in conjunction with Recital 20, it leaves no doubt that reference to 'equipment' is not confined to 'something materially substantial and solid' especially when considering the use of the term 'means' as opposed to 'equipment' in Recital 20 and other language version of the Directive.[919] In any case, the term 'equipment' must be given a broad interpretation. This is in accord to the rationale behind Art 4(1)(c): to prevent a controller that has its activities within EU from circumventing the protection afforded by the Data Protection Directive by relocating its place of establishment

[915] Ibid, p.95; see also Directive 95/46/EC, Recital 19.
[916] Ibid, p.93.
[917] Ibid, p.97.
[918] Bing, p.249, note 913,supra.
[919] See e.g., Bygrave, p.254, note 500, supra; Moerel, L., 'The long arm of EU Data Protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by website worldwide?', International Data Privacy Law, 2011, Vol.1, No.1, pp.28-46, at p.33.

outside the EU.[920] To further realize the spirit of Art 4(1)(c) and 'in order to ensure that the data subjects can effectively exercise their data protection rights against such a non-EU controller, Art 4(2) of the data Protection Directive subsequently provides that a non-EU controller that uses equipment on Community territory must designate a representative established on the territory of the relevant member State'.[921]

Many criticisms have been raised against Arts 4 generally and 4(1)(c) in particular. One of such criticisms is based on what is known as 'protection gap' i.e. a situation where certain matters are left unprotected by law. It is contended that Art 4(1)(c) provides for applicability of the Directive in situations where the controller is not established within EU.[922] However, Art 4(1)(a) does not apply in the reverse situation (that the controller is established within the EU) but applies only if the processing 'is carried out in the context of the activities of an establishment of the controller'.[923] The other criticisms raised is the possible rise of 'regulatory overreaching' in an online environment. By 'regulatory overreaching' it means a situation in which rules are expressed so generally and non-discriminatingly that they apply *prima facie* to a large range of activities without having much of a realistic chance of being enforced.[924] The frequently cited instance in which Art 4(1)(c) has been seen to have resulted into 'regulatory overreaching' by commentators is the operation of 'cookies'.[925] [926] The controversy which arises in relation to the application of 'cookies' by Websites' operators hinges around on 'cookies' from non-EU websites. Bygrave,[927] Kuner[928] and Moerel[929] share similar views that 'cookies' from non-EU websites should not be subject to the application of Art 4(1)(c) of the Directive lest 'regulatory overreaching' of the Directive will result. Yet, a different view has been consistently held by the

[920] Dammann, U and Smitis, S., EG-Datensschutzrichtlinie, Normos Verlagsgesellschaft, 1997, at p. 129 cited in Moerel, note 919, supra.
[921] Moerel, p.32, note 919, supra.
[922] Ibid, p.35.
[923] Ibid.
[924] Bygrave, p.255, note 500, supra.
[925] Ibid; see also Kuner, C., 'Data Protection Law and International Jurisdiction on the Internet (Part 2)', International Journal of Law and Information technology, 2010, Vol.18, No.3, pp.227-247, at p.229; Moerel, pp.39-43, note 919, supra.
[926] As to what are 'cookies'and how they function in respect to processing of personal information of individuals, see e.g., Zimmerman, notes 18,19 and 20 supra; Moerel, note 925, supra.
[927] Bygrave, note 924, supra-'If a Web site operator based in, say, India were to set "cookies" on to the browser programs of persons situated within the EU, then the operator's actions would arguably meet the criteria in Art 4(1)(c)-i.e. the operator would be processing personal data making use of equipment(broadly construed) situated on the territory of the EU Member State. This would mean that processing would be governed by the data protection law of the EU Member State concerned.'
[928] Kuner, note 925, supra.
[929] Moerel, p.40, note 919, supra.

Article 29 Working Party in several of its opinions.[930] In case of 'regulatory overreaching' or 'exorbitant jurisdiction'[931] in which case the jurisdictional scope of the law is much broader than the chance that the law will be enforced, there is a risk that respect for the law will be diminished.[932] The resulting low chance of enforcement may cause controllers to regard data protection rules as a kind of bureaucratic nuisance rather than as 'law'.[933] Much more complication in the application of Art 4 generally and 4(1)(c) in particular results from the recent development of 'cloud computing' technology.[934] In the 'cloud' it is difficult to locate the place of establishment of the controller or at least the scope of the activities of the establishment of the controller on a particular territory as such the data protection regime may be complicated to enforce.[935] This, as we shall see shortly, is among the reasons that made the revision of Directive 95/46/EC inevitable.

---

930 Article 29 Data Protection Working Party, 'Working Document on Processing of personal data on the Internet', 5013/99/EN/final, WP 16, (adopted on 23rd February 1999); Article 29 Data Protection Working Party, 'Working Document on Privacy on the Internet: An Intergraded EU Approach to Online Data Protection', 5063/00/EN/FINAL, WP 37, (adopted on 21st November 2000); Article 29 Data Protection Working Party, 'Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU based Websites', 5035/01/EN/Final, WP 56, (adopted on 30th May 2002), pp.10-12; Article 29 Data Protection Working Party, 'Opinion 1/2008 on Data protection Issues related to Search Engines', 00737/EN, WP 148, (adopted on 4th April 2008) and Article 29 Data Protection Working Party, 'Opinion 5/2009 on Online Social Networking', 01189/09/EN, WP 163, (adopted on 12th June 2009). It can be noted from this list that while most of these documents address issues of 'cookies' rather generally, WP 56 is very specific to such issues and similar technologies. Detailed comments on the Article 29 Working Party opinion over 'cookies' and related technologies in relation to applicability of Art 4(1)(c) are covered by Moerel, note 925, supra.

931 Kuner defines 'exorbitant jurisdiction' as improper or excess jurisdiction, see Kuner, p.227, note 925, supra.

932 Ibid, p.235.

933 Ibid, p.236.

934 The term 'cloud computing' has been variously defined by commentators. This thesis adopts the definition of Simon Bradshaw, Christopher Millard and Ian Walden as it is elaborative of the main feature of 'cloud computing' and neutral. According to these scholars, 'cloud computing' is defined in terms of three things: First, provision of flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand; second, abstraction and typical visualisation of services(especially infrastructure), by being generally allocated from a pool of shared as a fungible resource with other customers; and third, charging, where present, is commonly on an access basis often in proportion to the resources used; see Bradshaw, S *et al.*, 'Contracts for clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', International Journal of Law and Information technology, 2011, Vol.19, No.3, pp. 187-223, at p.189. This article is also appears as 'Queen Mary School of Law Legal Studies Research Paper No. 63/2010' at Social Science Research Network (SSRN), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 last visited 16/01/2012.

935 See e.g. Kuan Hon, W *et al.*, 'The Problem of "Personal Data" in Cloud Computing: What information is regulated?-the Cloud of Unknowing', International Data Privacy Law, 2011, Vol.1, No.4, pp.211-228; Dhillon, G and Kolkowska, E., 'Can a Cloud Be Really Secure? A Socratic Dialogue', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp.345-360; Ruiter, J and Warnier, M., 'Privacy Regulation for Cloud Computing: Compliance and Implementation in Theory and Practice', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp.361-376; Poullet, Y *et al.*, 'Data Protection in Clouds', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp.377-409; Casola, V *et al.*, 'Access Control in Cloud-on-Grid Systems: The *Perf*Cloud Case Study', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp. 427-444; Pieters, W., 'Security and Privacy in the Clouds: A Bird's Eye View', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp. 445-457, at p.452; Hustinx, P., 'Data Protection and Cloud Computing under EU Law', Third European Cyber Security Awareness Day BSA, European Parliament, 13 April 2010, pp.1-7, at pp.3-4 (Peter Hustinx is the European Data Protection Supervisor),

To address the above criticisms, commentators have advanced several recommendations. First, in order to reduce 'regulatory overreaching' Art 4(1)(c) has to be read down such that its application is limited to two situations: where the controller attempts to circumvent the law of an EU member state by relocating his/her/its establishment to a third country(but still uses means situated in the EU) and where the controller him-/her-/itself (who is located in a third country) transmits data to a third country for further processing(again using means situated in the EU).[936] Second, given the problem that data subjects have to cope with foreign legal systems in enforcing their rights, this could be remedied if applicable law were to be made the law of the State in which the data subject has his/her domicile.[937] Such a rule would parallel existing European rules on jurisdiction and choice of law in the case of consumer contracts.[938] Third, is the need for greater harmonization of the law; cooperation between regulatory authorities; technical solutions; development of a theory of comity or reasonableness and greater interaction between the jurisdiction and data protection worlds.[939] Interesting to note is that commentators have often addressed their solutions to choice of law issues as only means to 'reduce' such problems and not to completely eliminate them. This approach is sensible because it is practically difficult to completely eradicate choice of law disputes especially given the fact that: technology is constantly evolving; there are jurisdictions without completely data protection regimes which make it difficult to enforce the law there and even in those with such regimes there are still disparities in their formulation and implementation. With the upcoming of the EU General Data Protection Regulation, it is to be seen to what extent these recommendations have been taken on board. Also important to wait and see is how the Regulation is going to be put in practice. This is because, adopting a law is one thing yet its practice is another thing. The two may or may not match however well the laws are drafted.

f.) National Implementation

Any meaningful system of data protection law must be supported by a sound mechanism of its implementation. Such mechanism ensures that the rights and obligations of the data subjects and data controllers respectively are realized. To achieve this, Directive 95/46/EC requires every

---

http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf last visited 16/01/2012. Hustinx's views are that principles of EU law(including applicable law) remain relevant and fully applicable to the provision of cloud computing services- although there are some challenges in the way such principles apply, (see p. 6 of his speech).

[936] Bygrave, p.256, note 500, supra.

[937] Ibid.

[938] Ibid.

[939] Kuner, pp. 242-246, note 925, supra.

member state to establish one or more public authorities to monitor within its territory of the provisions of the national laws adopted by the member states under the Directive.[940] These authorities must act 'with complete independence' in exercising the functions entrusted to them.[941] The expression 'with complete independence' does not mean that such authorities should be established outside the government's structure. The independence referred here should be interpreted in the context of the functions of the authorities, hence functional independence. Care must be taken to ensure that the authorities' inevitable *dependence* on other bodies (e.g. through budget and personnel allocations) does not undermine the functional independence they are otherwise supposed to have.[942] Moreover, administrative and legal frameworks which leave open even a small possibility of a data protection authority being instructed by another administrative body on how to exercise its functions, most probably do not satisfy the criteria of Art 28(1).[943] Recently the meaning of 'with complete independence' has been a subject of a judicial dispute in *European Commission v Federal Republic of Germany,*[944] where in its judgment delivered on 9th March 2010 the European Court of Justice said:-

> 'In relation to public body, the term "independence" normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure. Contrary to the position taken by the Federal Republic of Germany, there is nothing to indicate that the requirement of independence concerns exclusively the relationship between the supervisory authorities and the bodies subject to that supervision. On the contrary, the concept of "independence" is complemented by the adjacent "complete", which implies a decision-making

[940] Directive 95/46/EC, Art 28(1).
[941] Ibid.
[942] Bygrave, p.70, note 24, supra; for detailed discussion as to how non-structural dependence affects the operation of the Data Protection Authorities see, Stewart, B., 'A Comparative Survey of Data Protection Authorities-Part1: Form and Structure', Privacy Law and Policy Reporter, 2004, Vol.11, No.2, http://corrigan.austlii.edu.au/au/journals/PLPR/2004/30.html last visited 19/03/2012; Stewart, B., 'A Comparative Survey of Data Protection Authorities-Part2: Independence and Functions', Privacy Law and Policy Reporter, 2004, Vol.11, No.3, http://corrigan.austlii.edu.au/au/journals/PLPR/2004/39.html last visited 19/03/2012; Kuner, C *et al.*, 'The Intricacies of Independence', International Data Privacy Law, 2012, Vol.2, No.1, pp.1-2; Greenleaf, G., 'Independence of Data Privacy Authorities(Part I): International Standards', Computer & Security Review, 2012, Vol.28, No.1, pp.3-13.
[943] Bygrave, note 942, supra.
[944] ECJ C-518/07.

> power independent of any direct or indirect external influence on the supervisory authority.'[945]

The rationale of the notion of 'complete independence' of supervisory authorities, was explained by the ECJ as follows:-

> 'The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions. It follows that, when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or the *Länder*, and not of the influence only of the supervised bodies.'[946]

It is intriguing to note that a 'mere risk' of the scrutinizing body that it may exercise political influence over the decisions of the supervisory authorities is sufficient to encroach the latter's 'independence' as clearly observed by the ECJ:-

> 'Furthermore, it should be pointed out that the mere risk that the scrutinizing authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks. First, as was stated by the Commission, there could be 'prior compliance' on the part of those authorities in the light of the scrutinizing authority's decision-making practice. Secondly, for the purposes of the role adopted by those authorities as guardians of the right to private life, it

[945] Ibid, Paragraphs 18-19; see also Raab, C.D., 'Roles and Relationships of Data Protection Authorities', Presentation at the Conference on 'The Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information 1995 – 2011' Budapest, 28 September 2011, pp. 1-24, http://abiweb.obh.hu/abi/abi_1995-2011/doc/Charles_D_Raab.ppt last visited 12/01/2012; European Union Agency for Fundamental Rights(FRA)., Data Protection in the European Union: the Role of the National Data Protection Authorities, Publications Office of the European Union, Luxembourg, 2010, pp.19-20.
[946] Ibid, Para 25.

> is necessary that their decisions, and therefore the authorities themselves, remain above any suspicion of partiality.'[947]

Another point clearly made out by the ECJ in this case is that the mode of appointment of the supervisory authorities either by executive or parliament does not *ipso facto* deprive such authorities of their statutory mandates of acting with 'complete independence' as envisaged under Art 28(1) of Directive 95/46/EC.[948] After taking all the above principles into account, the ECJ held the *Federal Republic of Germany* in breach of Art 28(1) 'by making the authorities responsible for monitoring the processing of personal data by non-public bodies and undertakings governed by public law which compete on the market (öffentlich-rechtliche Wettbewerbsunternehmen) in the different *Länder* subject to State scrutiny, and by thus incorrectly transposing the requirement that those authorities perform their functions 'with complete independence.'[949]

Within their 'complete independence' the data protection authorities are endowed with a wide range of functions and powers. Art 28(2) of the Directive puts a requirement that whenever administrative measures or regulations relating to protection of individuals' rights and freedoms with regard to processing of personal data are being drawn the supervisory authorities must be consulted. This requirement assumes that the supervisory authorities are staffed with personnel possessing technical expertise to be able to properly advise general and specific issues relating to administrative measures and regulations on processing of personal data. Apart from this advisory role, data protection authorities are also vested with power of investigation, of intervention and of engagement in legal proceeding and hear and determine complaints.[950] In the latter case the decisions of supervisory authorities may be appealed against through the courts.[951] The Directive also puts some obligations on supervisory authorities to ensure smooth discharge of functions

---

[947] Ibid, Para 36.

[948] Ibid, Paragraphs 43-46, the ECJ said, 'Admittedly, the absence of any parliamentary influence over those authorities is inconceivable. However, it should be pointed out that Directive 95/46 in no way makes such an absence of any parliamentary influence obligatory for the Member States. Thus, first, the management of the supervisory authorities may be appointed by the parliament or the government. Secondly, the legislator may define the powers of those authorities. Furthermore, the legislator may impose an obligation on the supervisory authorities to report their activities to the parliament. In that regard, a comparison may be made with Article 28(5) of Directive 95/46 which provides that each supervisory authority is to draw up a report on its activities at regular intervals which will then be made public. In view of the foregoing, conferring a status independent of the general administration on the supervisory authorities responsible for the protection of individuals with regard to the processing of personal data outside the public sector does not in itself deprive those authorities of their democratic legitimacy.'

[949] Ibid, Para 56.

[950] Directive 95/46/EC, Arts 28(3) and 28(4).

[951] Ibid, Art 28(3).

entrusted on them. Art 21(2) places the obligation to maintain a register of processing operations which may be inspected by any person. Also, the supervisory authorities are required to draw up reports at regular intervals.[952] Such reports are required to be public.[953] Under Art 28(7) members and staff of supervisory authorities are duty bound to maintain professional secrecy with regard to confidential information to which they have access during and after their employment has ended.

In the exercise of their powers to hear and determine complaints lodged to them, the supervisory authorities are empowered to impose sanctions and order compensation for damages. Although the Directive does not explicitly provide for imposition of sanctions and orders of compensation for damages such competence would clearly be compatible with the Directive.[954] In fact the Directive leaves specific details on sanctions, remedies and liability to be supplied by member states in their national data protection laws.[955]

g.) International Cooperation

Two sets of provisions can be identified under this sub-heading. First, there are those provisions in the Directive which create institutions or allocate functions to the institutions of the EU mostly those relating to supervisory duties over the implementation of the Directive. The second set relates to the relationships among the national supervisory authorities in member states.

Under the first category, the Directive establishes and/or allocates functions on four EU institutions: the Council of the European Union (or Council),[956] European Commission (or Commission),[957] Committee of Representatives of EU member states (or the Committee)[958] and

[952] Ibid, Art 28(5).
[953] Ibid.
[954] Bygrave, p.72, supra, note 24.
[955] Directive 95/46/EC, Arts 22, 23 and 24.
[956] Also informally known as the EU Council, this is where national ministers from each EU country meet to adopt laws and coordinate policies. This body should not be confused with: European Council – another EU institution, where EU leaders meet around 4 times a year to discuss the EU's political priorities or Council of Europe – not an EU body at all, see http://europa.eu/about-eu/institutions-bodies/european-commission/index_en.htm last visited 17/01/2012.
[957]The European Commission is one of the main institutions of the European Union. It represents and upholds the interests of the EU as a whole. It drafts proposals for new European laws. It manages the day-to-day business of implementing EU policies and spending EU funds. The Commission is composed of 27 Commissioners, one from each EU country providing the Commission's political leadership during their 5-year term. Each Commissioner is assigned responsibility for specific policy areas by the President; see http://europa.eu/about-eu/institutions-bodies/european-commission/index_en.htm last visited 17/01/2012.
[958] The Committee is established under Art 31 of Directive 95/46/EC.

the Article 29 Working Party.[959] The Commission is essentially the supervisory body as such it is required to report to the Council and the European Parliament at regular intervals on the implementation of the Directive.[960] The Commission's report may, where necessary contain as attachments, suitable proposals for amendments of the Directive taking into account of developments in information technology and in the light of the state of progress in the information society.[961] This report is required to be made public.[962] Moreover, the Commission is required to inform the Working Party, in a report, of the action it has taken in response to its opinions and recommendations.[963] Such report is further required to be forwarded to the Council and European Parliament.[964] It has to be made public.[965] Also, the Commission is required to enter into negotiations with third countries regarding the level of adequacy protection personal data as required in Art 25.[966]

The Committee, which is composed by representatives of the member states and chaired by the representative of the Commission, is mainly set up to assist the Commission.[967] The Committee is required under the Directive to render its opinion on drafts of measures proposed to be taken by the Commission.[968] In case of any disagreement, the matter has to be taken up by the Council for a decision.[969]

As already mentioned in previous sections, the Article 29 Working Party which is mainly composed of representatives of national supervisory authorities from each member state, is a 'technical group' which advises the Commission on a number of issues regarding the implementation of the Directive.[970] Most of its advice or recommendations may be given upon request by the Commission or on its own initiatives. Its opinion or decisions are not binding on the Commission.[971]

---

[959] The Article 29 Working Party is established under Art 29 of Directive 95/46/EC.
[960] Directive 95/46/EC, Art 33.
[961] Ibid.
[962] Ibid.
[963] Ibid, Art 30(5).
[964] Ibid.
[965] Ibid.
[966] Ibid, Art 25(5).
[967] Ibid, Art 31(1).
[968] Ibid, Art 31(2).
[969] Ibid.
[970] Ibid, Art 30(1) and 30(2).
[971] Ibid, Art 30(3).

The Directive also places obligation on part of the national supervisory authorities to cooperate with one another.[972] This cooperation is required to the extent necessary for the performance of their duties, in particular by exchanging all useful information.[973]

From the above, it can be submitted that in contrast to the *OECD Guidelines*, *Convention 108* and *UN Guidelines*, the Directive puts in place mechanisms to ensure harmonization of the Community's data protection regimes is achieved. However, whether this objective has been achieved or not is a different issue which needs to be examined (see 3.3.1.7).

3.3.1.7 General Data Protection Regulation 2012

The General Data Protection Regulation (GDPR) is the new data protection regime in Europe. It was officially announced on 25 January 2012 and was set to come into force two years after its publication. Since the Regulation was published in the Official Journal of the European Union on 20 February 2012 it was supposed to enter into force on 20 February 2014. The Regulation repeals Directive 95/46/EC and partly amends Directive 2002/58/EC. Although the review process that culminated to its adoption was officially launched in 2009, in reality the foundation of such process goes far back to numerous discussions, commissioned and non-commissioned reports, conference proceedings, commentaries by researchers, academics and practitioners, case law of the European Court of Justice, practices of national data supervisory authorities, etc between 1995 and 2009.[974] These sources provide clear signals that the Directive's revision was inevitable.

(a) Need for Regulatory Reforms

The revision of the Directive came about after one decade and a half of its adoption. Viviane Reding, the Vice-President of European Commission, EU Commissioner responsible for Justice, Fundamental rights and Citizenship has specifically pointed out three main trends as catalysts for

[972] Ibid, Art 28(6).
[973] Ibid.
[974] See e.g., European Commission Justice's Studies, Decisions, Reports and Surveys, http://ec.europa.eu/justice/data-protection/document/index_en.htm last visited 18/01/2012; Article 29 Working Party on data Protection 1st, 2nd, 3rd, 4th, 5th ,6th , 7th ,8th ,9th ,10th ,11th ,12th and 13th Annual Reports, http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/index_en.htm last visited 18/01/2012; Article 29 Working Party on Data Protection's Opinions, Working Documents and Recommendations(1997-2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm last visited 18/01/2012; also see various publications previously referred in this thesis making general or specific comments on Directive 95/46/EC.

regulatory reforms: modern technologies, globalized data flows and access to personal data by law enforcement authorities.[975] As regards modern technologies-the growth in mobile Internet devices, web-user generated contents, the outburst of social networking sites and above all the cloud computing technologies have been identified as new trends which postdate the Directive 95/46/EC. Because the latter law was adopted while the Internet was just at its embryonic stages in 1990s, the recent technological developments have strained its operation. The modern technological developments have in turn increased globalised data flows at a 'rocketing' rate. Accordingly, globalization of technology has seen an increased role of third countries relating to data protection, and has also led to a steady increase in the processing of personal data of Europeans by companies and public authorities outside the European Union.[976] As a result, it has been difficult to precisely allocate responsibility, liability and accountability of various parties notably data controllers, processors as well as joint data controllers and processors. Also these cross-border flows of data to third countries have posed great challenges on how Europeans can enforce their data protection rights in non-EU jurisdictions. Besides these two trends, the growing appetite for personal data for reasons of public interest, in particular for public security matters, is also an important challenge for data protection.[977] While 'the collection and processing of personal information can be very valuable in order to secure important and legitimate public and public interests-if done in a way which fully respects the requirements of legality, necessity, and proportionality',[978] its reverse may be disastrous to individuals' control of their personal data.

The totality of the above trends exerted pressure to the need for revising the Directive. Such revision aimed at achieving the following objectives: strengthening the rights of data subjects; enhancing the internal market dimension; reinforcing data controllers' responsibility; revising the rules on police and judicial cooperation in criminal matters; improving, strengthening and streamline the current procedures for international transfers in the context of global dimension of data protection and providing better enforcement of data protection rules.[979]

---

[975] Reding, V., 'The Upcoming Data Protection Reform for the European Union', International Data Privacy Law, 2011, Vol.1, No.1, pp.3-5, at p.3.
[976] Ibid.
[977] Ibid.
[978] Ibid.
[979] Ibid, pp.3-5;see also, European Commission., 'A Comprehensive Approach on Personal Data Protection in the European Union', COM (2010)609 final, Brussels, 4 November 2010, pp.1-19, at pp.5-16.

(b) Review Process

The review process of Directive 95/46/EC has to be viewed broadly in the light of discussions, assessments, comments, recommendations and practices of EU member states as analysed by academics, practitioners, researchers, Article 29 Working Party, the Commission, etc between 1995 and 2009. However it is imperative to highlight the formal review process that led to the adoption of the Regulation. This is important for a number of reasons. First, it helps to understand which stages were involved; second, examining the review process shows who were involved in the process and how competing interests were identified and resolved; third, the examination may also shed some light to what extent the review process was transparent; fourth and especially for non-EU countries which may or may have not enacted data protection legislation, the examination of the review process may provide a lesson for legal reforms when reviewing or adopting their legislation. However this does not suggest that the EU review process approach is the best model to be followed. Non-EU countries, while following their legal reform traditions, may still learn from EU because the latter has relatively longer experience in data protection law practices and in fact the adoption of most data protection legislation in such non-EU countries were inspired by Europe.

- **The Korff and Brown Report 2010**

The Directive 95/46/EC formal review process was initiated by the European Commission by commissioning a study: 'New Challenges to Data Protection'.[980] This study is commonly known as Korff and Brown Report 2010 after the names of its lead consultants Professor Douwe Korff of the London Metropolitan University and Professor Ian Brown of the University of Oxford-Oxford Internet Institute. A special team of experts who provided assistance to the lead consultants included: Professor Peter Blume (University of Copenhagen, Denmark), Professor Graham Greenleaf (University of New South Wales, Sydney, Australia), Chris Hoofnage-Senior Fellow(University of California, Berkeley, California, USA), Lilian Mitrou-Assistant Professor (University of the Aegean, Mytilene, Greece), and Filip Pospíšil, Helena Svatošová, Marek Tichy-researchers(NGO *Iuridicum Remedium*, Prague, Czech Republic). Also in the team were advisors: Professor Ross Anderson (University of Cambridge, UK), Caspar Bowden (Microsoft

[980] European Commission DG Justice, Freedom and Security., 'Comparative Study on Different Approaches to New Privacy Challenges, in particular in the light of Technological Developments', Contract Nr: JLS/2008/C4/011-30-CE-0219363/00-28; Final Report, 20 January 2010,ttp://papers.ssrn.com/sol3/papers.cfm?abstract_id=1636706 last visited 18/01/2012.

Corporation, UK), Professor Katrin Nyman-Metcalf (University of Tallinn, Estonia) and Paul Whitehouse (Former Chief Constable, Head of Police Force, Sussex Police (rtd), UK).

The study leading to the Korff and Brown Report was carried out from October 2008 to August 2009. However the final report of the study was preceded by an Inception and Interim Reports submitted in December 2008 and March 2009 respectively. The purpose of the Korff and Brown study was to identify the challenges for protection of personal data produced by current social and technical phenomena such as the Internet; globalization, the increasing ubiquity of personal data and personal data collection; the increasing power and capacity of computers and other data-processing devices; special new technologies such as RFID, biometrics, face-(etc) recognition, etc; increased surveillance (and 'dataveillance) and increased uses of personal data for purposes for which they were not originally collected, in particular in relation to national security and the fight against organized crime and terrorism.[981] The other purpose of the study was to produce a report containing a comparative analysis of the responses that different regulatory and non-regulatory systems (within the EU and outside it) offer to those challenges.[982] Finally, it was the purpose of the study to provide guidance on whether the legal framework of the main EC Directive on data protection (Directive 95/46/EC) still provides appropriate protection or whether amendments should be considered in the light of best solutions identified.[983]

In response to the three main purposes of the study, the Report has revealed that at the bottom of the challenges inhibiting the effectiveness of the application of the Directive to its desired goals are two interwoven strands: the challenges caused by technical developments and those resulting from social and political changes and choices.[984] Accordingly the study has found that the exponential increases in technologies and their sophistication have radically increased the ability of organizations to collect, store and process personal data.[985] Illustrations provided by the Report include CCTV, mobile phone technology, biometric and electronic identifiers. Also individuals are using social networking sites to share information about themselves and their family, friends and colleagues.[986] Similarly, governments are increasingly analyzing and

[981] Ibid, p.9 (Para 3).
[982] Ibid.
[983] Ibid.
[984] Ibid, p.12 (Para 6).
[985] Ibid, (Para 7).
[986] Ibid, (Para 8).

exchanging information on their citizens in response to fears of terrorist attacks.[987] Moreover, it has been found that both technology and government policies have tended to globalize data collection and dissemination and to diffuse data storage.[988]

The Korff and Brown Report has pointed out a number of limitations of the current Directive to address the above challenges. Some matters brought about by the technological developments as well as social and political changes and choices have fallen outside the Directive or national laws implementing it.[989] Those exclusions are more problematic in the new Web 2.0 environment in particular.[990] There are also still major conflicts of law, even within the EU/EEA, but especially in relation to controllers in non-EU/EEA countries; and these conflicts will grow strongly.[991] The study further discovered wide difference in the application and interpretation of basic data protection concepts and rules, within the EU/EEA, and wide differences still between EU/EEA and other countries; in a generally-internationalized world of data processing, these differences will be increasingly problematic.[992] These differences are partly due to inadequate or deficient implementation of the Directive and partly due to differences in interpretation of the Directive.[993] It has been noted by the study that the EU Commission has not sufficiently forcefully pursued enforcement action against member states that have not properly implemented the Directive.[994] Also, the mechanisms in the Directive which were laid down with the aim of achieving greater harmonization have not been sufficiently used. In some instances such procedures and mechanisms were found to be deficient in themselves.[995] With regard to the findings of 'adequacy' the Report revealed that the EU Commission has used the procedure to issue 'adequacy findings' in only limited number of countries.[996] Globally, the procedure has therefore had a more limited impact than would have been hoped; and the development of strong data protection laws in non-U/EEA countries has consequently been less strongly promoted than that might have been the case.[997] Even in the EU/EEA, enforcement by the national Data Protection Authorities is not strong or comprehensive. Enforcement in non-European countries including the USA is even weaker.[998] Supplementary and alternative means

[987] Ibid.
[988] Ibid, p.14, (Para 12).
[989] Ibid, p.16, (Para 17).
[990] Ibid.
[991] Ibid.
[992] Ibid.
[993] Ibid.
[994] Ibid.
[995] Ibid.
[996] Ibid.
[997] Ibid.
[998] Ibid.

to enhance data protection, including technical means such as encryption, anonymisation, identity management tools and other PETs-are still rather undeveloped, often weak in their implementation and effect.[999] Despite all these limitations, the study found that the challenges highlighted above have effect to matters of application; interpretation and effectiveness of enforcement/assumption of rights: the basic data protection principles are not challenged, but rather, need reasserting and fuller practical application.[1000]

The major recommendations of the Korff and Brown Report include the following. First, the Report recommends for the review of the Directive. However it recommends further that data protection law in the EU should continue to rest on the basic data protection principles and-criteria set out in the Directive 96/46/EC.[1001] While the application of these broad standards needs to be clarified they themselves do not require major revision in order to meet the new challenges.[1002] The Report also recommends the abolition of the pillar system in the Directive especially for matters falling under the first and third pillars as the issues governed in each of these pillars are increasingly intertwined with each other.[1003] With regard to the matters of 'applicable law' the Report recommends the same to be based upon the 'country of origin' principle (as contained in the Original proposals of the Directive)[1004] as opposed to the current 'territoriality principle'. The radical recommendation of the Report as to issues of harmonization of substantive law is the replacement of the main Directive with a (directly applicable) Regulation (something that had been originally considered in the drafting of the main Directive).[1005] The recommendation on cooperation with non-EU/EEA countries, especially the 'adequacy' finding is rather vague, but adds the possibility of adopting a system of 'provisional rulings' as the current procedure takes long.[1006] With regard to supervisory and enforcement, the Report recommends that there should be 'prior checking' of all population-scale systems in the member state.[1007] On matters of individual rights and remedies the Report recommends that individuals should be able to obtain effective redress, as well as interim and permanent injunctions, in speed, simple and cheap processes before competent, independent and impartial fora.[1008] Finally, the

[999] Ibid, pp.16-17,(Para 17).
[1000] Ibid, p.17, (Para 18).
[1001] Ibid, p.21, (Para 27).
[1002] Ibid.
[1003] Ibid, p.22, (Para 30).
[1004] Ibid, p.26, (Para 44).
[1005] Ibid, p. 39, (Para 90).
[1006] Ibid, p. 43, (Para 103).
[1007] Ibid, p.45, (Para 108).
[1008] Ibid, (Para 110).

Report recommends use of supplementary and alternative measures to protection of personal data.[1009] Such means include for example the Privacy Enhancing Technologies (PETs).

- **May 2009 Stakeholders' Conference on Data Protection**

Subsequent to receipt of the Interim Korff and Brown Report in March 2009, the European Commission organised a conference and the same was held in Brussels in Belgium from 19 to 20 May 2009.[1010] The theme of the conference was 'Personal data - more use, more protection?' The purpose of the conference was to give opportunity to various stakeholders to express their views and questions on the new challenges for data protection and need for an information management strategy in Europe.[1011] Moreover the Conference formed part of the Commission's open consultation on how the fundamental right to protection of personal data could be further developed and effectively respected, in particular in the area of freedom, justice and security.[1012] Some of the papers presented and discussed in the Conference touched upon issues such as: profiling, transparency and notification in the age of Internet, role of supervisory authorities and rights of data subjects, awareness and public opinion, globalisation, digital data protection and issues of freedom of information.[1013]

- **First Public Consultation**

As a follow-up to the Data Protection Conference held on 19-20 May 2009 in Brussels, the European Commission launched a wider public consultation in July 2009.[1014] The official title of the consultation was: 'Consultation on the legal framework for the fundamental right to protection of personal data.'[1015] The period of the consultation was set from 9 July 2009 to 31 December 2009.[1016] The objective of this consultation was to obtain views on the new challenges

[1009] Ibid, p.46, (Para 114).
[1010] European Commission., 'Personal data-more use, more Protection?' Press Release from the Commission inviting stakeholders to register and attend the Data Protection Conference, 19-20 May 2009, in Brussels, Belgium, http://ec.europa.eu/justice/news/events/conference_dp_2009/press_release_en.pdf last visited 18/01/2012.
[1011] Ibid.
[1012] Ibid.
[1013] Ibid.
[1014] European Commission., 'Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data' Brussels, 4 November 2010, pp.1-22, at p.2;
http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf last visited 18/01/2012.
[1015] European Commission Website,
http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm last visited 18/01/2012.
[1016] Ibid.

for personal data protection in order to maintain an effective and comprehensive legal framework to protect individual's personal data within the EU.[1017]

In this public consultation, the Commission asked three main questions to wit: please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation; in your views, the current legal framework meets these challenges?; and what future action would be needed to address the identified challenges?[1018] In response to these questions, the Commission received 168 responses, 127 from individuals, business organisations and associations and 12 from public authorities.[1019]

- **Second Public Consultation**

Based upon the Korff and Brown Report, stakeholders' views collected from the Conference on Data Protection: May 2009 and the First Public Consultation published at 'Your Voice in Europe', the European Commission developed 'A Comprehensive Approach on Personal Data Protection in the European Union.'[1020] The Commissioner's proposed approach was put into the second public consultation: 'Consultation on the Commission's comprehensive approach on personal data protection in the European Union.'[1021] The period of consultation was scheduled from 4 November 2010 to 15 January 2011.[1022] The objective of the consultation was to obtain views on the Commission's ideas - as highlighted in the Communication attached to the consultation - on how to address the new challenges for personal data protection (e.g. fast developing technologies and globalisation).[1023] It aimed to ensure an effective and comprehensive protection of individual personal data within the EU.[1024] The total number of responses received to this consultation was 305.[1025] 54 responses were received from individuals (citizens), 31 from public authorities and 220 responses were received from private organization (business associations and non-governmental organizations).

[1017] Ibid.
[1018] Ibid.
[1019] European Commission, note 1014, supra. Note that the confidential responses are not included in this list.
[1020] European Commission., pp.1-19, note 979, supra.
[1021] European Commission Website,
http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm last visited 18/01/2012.
[1022] Ibid.
[1023] Ibid.
[1024] Ibid.
[1025] Ibid (note that only 288 responses are indicated on the Commission's Website. But the full number of responses of 305 appears in the Explanatory Memorandum to the First Draft Proposal of the Regulation, p.2).

- **Approval of the Commission's Approach on Personal Data Protection**

By its unanimously adopted resolution of 6 July 2011, the European Parliament approved the Commission's approach to reforming the data protection framework in Europe.[1026] Earlier on 24 February 2011 the Council of the European Union had adopted its conclusions in which it broadly supported the Commission's intention to reform the data protection framework and agreed to many elements of the Commission's approach.[1027] Similar expressions of support came from the European Economic and Social Committee.[1028]

- **Surveys, Targeted Consultations, Seminars and Conferences**

The review process also included surveys, the most important one being the Eurobarometer Survey held in November-December 2010 in which European citizens were consulted on number of issues regarding privacy and data protection.[1029] Apart from the Korff and Brown which was a specifically commissioned study into issues which came to be the foundation of the Commission's approach to the revision of the Directive, other studies were parallel launched.[1030] Also important to mention is that throughout 2010 and 2011, various targeted and specific consultations (apart from the two public consultations) were conducted with key stakeholders-member state authorities, private stakeholders, as well as privacy, data protection and consumers' organizations.[1031] Moreover there were a series of dedicated workshops and seminars on specific issues held in 2011.[1032] Conferences were similarly organized during the review period. Three of these conferences deserve mention. The first was a co-organized high level conference by the European Commission and the Council of Europe on 28 January 2011(Data Protection Day).[1033] In this conference various issues related to the reform of the EU legal framework as well as the need for common data protection standards worldwide were discussed. The second and third

[1026] European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI))http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=EN&ring=A7-2011-0244 last visited 19/01/2012.
[1027] Explanatory Memorandum to the First Draft Proposal of the Regulation, p.5.
[1028] Ibid.
[1029] European Commission, 'Attitudes on Data Protection and Electronic Identity in the European Union', Special Eurobarometer 359, November-December 2010,
http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf last visited 19/01/2012.
[1030] Explanatory Memorandum to the First Draft Proposal of the Regulation, p.4.
[1031] Ibid.
[1032] Ibid.
[1033] Ibid.

conferences on data protection were hosted by the Hungarian and Polish Presidencies of the Council on 16-17 June 2011 and on 21 September 2011 respectively.[1034]

- **Adoption of the Regulation**

The review of Directive 95/46/EC was expected to come to an end with the adoption of the Regulation by the European Parliament and the Council. However, it is not certain when the Regulation will be adopted as it is still a work in progress.

(c) Main Elements of the Regulation

Like its predecessor, the Data Protection Regulation is grounded on the same philosophical basis and objectives as the Directive i.e. human rights philosophy and accordingly the twin objectives of the Regulation are to protect fundamental rights and freedoms of natural persons particularly their rights to protection of personal data and to ensure free flow of information within the European Union. Similarly the scope of the Regulation has remained the same as the Directive. It applies, as at its initial point, on processing of personal data of natural person in both public and private sector regardless of the technology employed.[1035] This means both manual and automatic processing of personal data are covered by the Regulation. Structurally, the Regulation is a longer and more detailed text than the Directive. The former has a preamble containing one hundred and eighteen recitals. It also contains eleven chapters with a total number of ninety one Articles.

The central element of the Regulation is its retention of the basic principles of data protection in Directive 95/46/EC. However to make such principles apply smoothly, additional elements are introduced notably the transparency principle, clarification of the data minimization principle and establishment of a comprehensive responsibility and liability of the controller.[1036] The criteria of lawful processing have remained the same as in the Directive only that the balance of interest criterion has to be applied. Also the Regulation clarifies the conditions regarding re-purposing of the processing as well as conditions of consent with regard to processing of personal data.

[1034]Ibid.
[1035] Regulation, Arts 1 and 2.
[1036] Explanatory Memorandum to the First Draft Proposal of the Regulation, p.8.

On issues of data subject's rights, the Regulation retains same rights as the Directive. However their scope has been far clarified. The principle of transparency is at the root of the exercise of such rights. It is interesting to note in this regard that the Regulation has introduced a new right, '*the right to be forgotten*' which simply mandates a data subject to direct the controller or processor, as the case may be, to erase and destroy completely any information relating to him or her, especially when its purpose or period required has expired or consent has been withdrawn.

The Regulation clarifies issues of controller and processor's obligations in data processing. Joint data controllers are also clarified. It is imperative to note that the Regulation introduces in clear terms the 'principle of accountability' as an obligation on the part of data controllers and processors. Controllers and processors are also obliged to carry out a data protection impact assessment prior to risky processing operation. Also important to note is that the Regulation puts obligation on data controllers and processors to employ Data Protection Officers (DPO) whom will be required to possess knowledge on issues of data protection law and regulations. The officer is required to discharge his or her duties with some levels of independence.

The general principles of trasnborder flow of personal data to third countries and international organizations are still maintained by the Regulation. The criteria and procedures for the adoption of an 'adequacy' decision by the Commission are based on Arts 25 and 26 of the Directive: rule of law, judicial redress and independent supervisory authority. However, the Regulation makes it clear that there is a possibility for the Commission to assess the level of protection afforded by a territory or a processing sector within a third country. Also binding corporate rules and standard contractual clauses are clearly spelt as means to be considered in the 'adequacy' assessment of data protection levels in third countries.

Choice of law rules have been radically changed in the Regulation. While in the Directive, the choice of law rules were based upon the 'territoriality principle' in the Regulation, such rules are based upon the 'country of origin' principle.

The Regulation clarifies a number of enforcement measures to be available for data subjects to enforce their rights. Sanctions and compensations have been enhanced. Previously the Directive did not clarify these issues as they were only left to the member states to provide them in their national data protection legislation.

Some definitions in the Directive have been taken out from the Regulation. Others have been retained by being complemented with additional elements in order to broaden their scope or to clarify them. In some instances, completely new definitions not part of the Directive have been introduced in the Regulation. Most of these definitions have been dealt with in such ways they address the challenges of modern technologies.

The Regulation has replaced the Article 29 Working Party with the European Data Protection Board. Yet the Board is similarly composed of representatives (i.e. heads) of national supervisory authorities of each member state. Members of the Commission are no longer part of the Board, although they may attend its meetings, etc. The Regulation clarifies the independence of the Board, and describes its responsibilities and roles.

Finally, and as its name suggests, the Regulation has a binding force upon EU/EEA member states and direct effect on them. The rationale for adopting a Regulation instead of a Directive (which has to be implemented or transposed by each member) is to achieve harmonization of the rules and practices.

(d) Regulation's Implications

The implications of the Data Protection cannot be fully drawn at this stage. As pointed out, any assessment of the impact of a law depends on a vast array of factors-chiefly among them is sufficient practice of the law itself. Since the Regulation is still a work in progress, any thorough assessment on how it will actually function in practice is premature. Yet, some minimum assessment can still be made especially on provisions which were retained by the Regulation from the Directive and whose adjustments are not radical. This thesis limits early assessment to matters of transfers of data to non-EU/EEA countries (i.e. third countries) for two reasons. First, the provisions on transfer of personal data to third countries incorporated in the Regulation (i.e. Arts 37 and 38) have ramifications on legal reforms to third countries including sub-Saharan Africa (the focus of the present thesis). Second, the third research question of this study is built upon transborder flows of data from Europe to third countries, accordingly it is important to comment on those provisions. Also important to bear in mind is that the provisions on 'adequacy' in the Regulation are patterned to Arts 25 and 26 of the Directive. However in making preliminary assessment one difficult must be revealed. The primary criterion of transfer of personal data to third countries originating from EU/EEA is the 'adequacy' level

of protection of personal data afforded by a third country in question. However, when assessing whether such 'adequacy' standard is met, automatically the other provisions of the Regulation (both substantive and procedural) have to be considered. Aware of this imminent risk, it is important to limit as low as possible thorough assessment of the provisions of the Regulation on TBDF. Suffice to point that non-EU/EEA countries or specific sectors within such countries which had already been declared by the Commission as providing adequate level of data protection may find themselves required to revise their laws or principles in line with the Regulation. Moreover those third countries which are still under the process of 'clearance' are likely to be provided with additional criteria in adjusting their laws. It remains to be seen what effect the Regulation will bring about to third countries when it comes into application.

3.3.2 U.S.-EU Safe Harbor

The U.S.-EU Safe Harbor Framework (SH) is an agreement negotiated between the two sides of the Atlantic with the view of sustaining continued flow of personal information on both sides.[1037] The context in which the SH came about can be explained in the requirements of the European Data Protection Directive 95/46/EC that any international transfer of personal data to non-EU/EEA countries (the so called 'third countries') should meet the 'adequacy' test under Arts 25 and 26 lest flow of information to such foreign destinations should be stopped. Since the United States fall outside EU/EEA, it became a direct victim of the 'adequacy' requirement. Given that U.S.A and Europe have two conflicting philosophies and approaches to privacy protection, which in any case it would be difficult to reconcile, negotiation for a compromise to take into account these varying approaches became necessary.

As seen above, the European approach towards data protection is grounded in the concept of privacy as a fundamental human right.[1038] In this conception, a just and free society results only when individuals are able to interact with self-determination and dignity.[1039] Accordingly, Europe has always taken a proactive role to comprehensively regulate the protection of personal data through national legislation even prior to Directive 95/46/EC. The United States' approach is sharply different. Americans tend to be more trusting of the private sector and the free market to

[1037] Safe Harbor Policy Principles, http://export.gov/safeharbor/eu/eg_main_018475.asp last visited 21/01/2012.
[1038] Long, W.J and Quek, M.P., 'Personal Data Privacy Protection in an Age of Globalisation: the US-EU Safe Harbor Compromises', Journal of European Public Policy, 2002, Vol.9, No.3, pp.325-344, at p.331.
[1039] Ibid.

protect personal privacy-fearing more the invasion of privacy from the state not the market.[1040] In the latter case it has generally been viewed that a 'marketplace of ideas' allows only minimum restrictions on flows of information, including personal information.[1041] Driven by market philosophical ideals, the United States has dealt with privacy protection from an *ad hoc* sectoral approach.[1042] This legislative approach to protection of privacy has never changed despite the increasing rate and amount of personal information processed by public and private sectors and also individuals as a result of modern technologies. Instead, U.S.A has up to present resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector.[1043] From the EU point of view, and even from the Americans self-assessment, the latter's approach to protection of personal data would not be adequate within the meaning of Arts 25 and 26 of the Directive even prior to any assessment and assigning the 'adequacy' label.

Apart from the contrasting legislative philosophies behind privacy protection, the compromise of EU-U.S standards forging SH has to be broadly viewed from an economic perspective. Both EU and U.S are the world's two most powerful and highly independent, economic entities.[1044] Together, the European Union and United States account for over one-half of world GDP.[1045] The EU is the United States' largest trading partner: in 1999(one year after Directive 95/46/EC became operational) the United States had US Dollar 350 billion in trade with the EU.[1046] Moreover U.S-controlled affiliates based in Europe sell an even greater quantity of goods and services-estimated at US Dollar 1.2 trillion.[1047] These U.S firms were most vulnerable to a potential restriction on transborder data flow.[1048]

[1040] Ibid.
[1041] Reidenberg, J.R., 'Setting Standards for Fair Information Practices in the US Private Sector', Iowa Law Review, 1995, Vol. 80, No.3, pp.497-552, at p.499.
[1042] See e.g., Fair Credit Reporting Act 1970; Cable Communications Policy Act 1984; Electronic Communications Privacy Act 1986; Video Privacy Protection Act 1988; Telecommunications Act 1996; Children's Online Privacy Act 1999; Grammm-Leach-Billy Act 1999. In contrast to the *ad hoc* approach to privacy protection in the private sector, the United States has general privacy legislation and specific legislation regulating the public sector, see e.g., the Privacy Act 1974; Family Educational Rights and Privacy Act(FERPA) 1974; Right to Financial Privacy Act 1978; Privacy Protection Act 1980; Computer Matching and Privacy Protection Act 1988(amending the Privacy Act 1974); Driver's Privacy Protection Act 1994; Health Insurance Portability and Accountability Act 1996.
[1043] Reidenberg, p.500, note 1041, supra.
[1044] Long and Quek, p.326, note 1038, supra.
[1045] Ibid.
[1046] Ibid.
[1047] Ibid.
[1048] Ibid; see also Hobby, S.P., 'The EU Data Protection Directive: Implementing a Worldwide Data Protection Regime and How the U.S Position has progressed', International Law & Management Review, 2005, Vol. 1, pp.155-190, at p.180.

(a) Negotiating Safe Harbor Framework

Formal discussions between EU and U.S.A on Safe Harbor started in 1998 six months earlier than the official date the Directive became operational. In these discussions, the United States was represented by the U.S Department of Commerce while for the European Union, the role was played by the European Commission. The competence of these two bodies was called into question.[1049] Yet, they went ahead to the finalization of the SH. However contrary to the previous or subsequent approach, the finding of U.S.A as providing 'adequate' level of protection of personal data in the context of SH did not end with the European Commission. It also required consultations and/or decisions from the Article 31 Committee, Council of the European Union as well as the European Parliament.

The SH discussions involved chiefly direct discussions and exchange of letters. There were many challenges in the negotiation process reflecting various interests at stake. Initially, discussions were frustrating.[1050] The European Union maintained that it was interested only in legislation drafted to provide adequate protection to the data of European citizens which had been exported, while the U.S sought to postpone the implementation of the Directive, and to gain recognition of adequacy for the U.S system as it then stood.[1051] However, a suggestion by David L. Aaron (Undersecretary of Commerce for International Trade) that the adequacy judgment need not extend to the entire U.S system, but rather to a set of firms which had voluntarily agreed to embrace a set of privacy principles, provided to be the basis for a potential compromise.[1052] Nonetheless, the principles of privacy proposed by U.S.A to EU were continued to be put under scrutiny for more than a year later.[1053]

Other interests which operated for or against SH discussions came from the domestic politics within the U.S itself.[1054] The main contending groups were the U.S administration, concerned

---

[1049] See e.g., Hubbard, A., 'Does the Safe Harbor Agreement have a future? If so, what kind?', A Tutorial Paper presented at the Norwegian Research Centre for Computers and Law (NRCCL), Spring, 2006, pp.1-10, at p.2.
[1050] Farrell, H., 'Negotiating Privacy across Areanas: The EU-US "Safe Harbor" Discussions' in Héritier, A(ed)., Common Goods: Reinventing European and International Governance, Rawman & Littlefield, Boulder/New York/Oxford, 2002, pp.101-123, at p.107.
[1051] Ibid; It is highly unlikely if U.S would pass the adequacy test, see e.g., Murray, P.J., 'The Adequacy Standard under Directive 95/46/EC: Does U.S Data Protection Meet This Standard?', Fordham International Law, 1997, Vol. 21, No.3, pp.931-1018.
[1052] Ibid.
[1053] For sequences of negotiations of SH see e.g., Heisenberg, D., Negotiating privacy: the European Union, the United States, and personal data protection, Boulder/Colo. : Lynne Rienner Publishers, 2005, Chapter four (4).
[1054] Farrell, p.109, note 1050, supra.

businesses and business organizations, and consumer groups.[1055] In the interest of e-commerce, the administration generally advocated a hardline position which would seek to force the EU to back down.[1056] Although with some division, the business which had/has strong relationship with the U.S administration lobbied heavily while the Directive was working its way through the EU decision-making process. It had been successful in persuading lawmakers to water down some of its requirements.[1057] The U.S consumer organizations favoured strong legislation to protect individual privacy, both in the online and offline worlds.[1058] Also important to note is that the other set of interests for or against SH came from within the European Union itself.[1059] The Commission was interested to negotiate with the United States in order to try to reach an adequacy finding which would allow firms to comply with the Directive.[1060] This interest seems to have been developed out of fear that many firms in the EU would ignore the Directive and continue to transmit personal information to the United States, because it was necessary to their business, and because the benefits outweighed the risks of being caught.[1061] In any case, this would have undermined the intent and credibility of the Directive.[1062] Similarly, member states had different position. For example, the UK and Ireland had no difficulties in principle with a self-regulation, non-legislative compromise of the sort that finally emerged.[1063] Germany and France, in contrast were more skeptical about self-regulation, and more difficult to persuade.[1064] The European Parliament was also split.[1065] A lot of concerns were raised on the effectiveness of self-regulation to offer adequate protection of personal data. There was finally the Article 29 Working Party which, although advisory body in its role, it has influence on the decisions of the European Union institutions particularly the European Commission. The Working Party was

[1055] Ibid, p.110.
[1056] Ibid, p.111.
[1057] Regan, P., 'American Business and the European Data Protection Directive: Lobbying Strategies and Tactics', in Bennett, C and Grant, R (eds)., Visions of Privacy, University of Toronto Press, Toronto, 1999 cited in Farrell, note 1056, supra.
[1058] Farrell, note 1056, supra.
[1059] Ibid, p.109.
[1060] Ibid.
[1061] Ibid.
[1062] Ibid.
[1063] Ibid.
[1064] Ibid; it is also interesting to note that in 2010(almost ten years after the adoption of SH have lapsed) Germany Data Protection Authorities (DPAs) decided that data exporters may not exclusively rely on the Safe Harbor List in determining if U.S. data importers afford an adequate level of protection to personal data. The decision was taken on April 28/29, 2010, in the so-called *Düsseldorfer Kreis*, which is a joint working committee of all German DPAs. According to the decision, German data exporters must carry out certain minimum checks to ensure that the chosen data importer is not only formally self-certified but also adheres to the Safe Harbor Principles in practice. Data exporters who fail to carry out such checks can be held liable and might face sanctions in the absence of an adequate level of data protection at the U.S. data importer's end, see Schmidl, M and Krone, D., 'Germany DPAs Decide EU-U.S. Safe Harbor May Not Be Relied Upon Exclusively', http://www.bnai.com/GermanyDpas/default.aspx last visited 24/01/2012; This article appeared first on World Data Protection Report in May 2010 issue.
[1065] Farrell, note 1055, supra.

deeply skeptical of the proposition the 'patchwork of narrowly-focused sectoral laws and voluntary self-regulation' that characterized the U.S could provide comprehensive protection to the data of European citizens.[1066] It is unsurprising to find that, throughout i.e. before, during and after the adoption of SH, the Article 29 Working Party had/has always found the U.S providing inadequacy level of protection of personal data.[1067]

SH took nearly two years of negotiations. The full agreement came into existence in 2000. It comprises two sets of documents. The first set includes documents issued by the United States and published in the Federal Register on 24 July 2000 and 19 September 2000.[1068] The second set includes documents published by the European Commission on 28 July 2000.[1069] The other documents which are part and parcel of the SH Framework are the European Commission's finding of adequacy, exchange of letters between the U.S Department of Commerce and the European Commission on specific issues such as enforcement, and letters from the U.S Department of Transportation and Federal Trade Commission on the agencies' powers to enforce the policy.[1070]

[1066] Ibid.

[1067] See e.g., Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, 5092/98/EN/final, WP 15, (adopted on 26th January 1999); Opinion 2/99 on the Adequacy of the 'International Safe Harbor Principles' issued by the U.S Department of Commerce on 19th April 1999, 5047/99/EN/final, WP 19, (adopted on 3rd May 1999); Opinion 4/99 on the Frequently Asked Questions to be issued by the U.S Department of Commerce in relation to the proposed 'Safe Harbor Principles', 5066/99/EN/final, WP 21, (adopted on 7th June 1999); Working Document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning 'the International Safe Harbor Principles', 5075/99/EN/final, WP 23, (adopted on 7th July 1999); Opinion 7/99 on the Level of Data Protection provided by the 'Safe Harbor' Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the U.S Department of Commerce, 5146/99/EN/final, WP 27, (adopted on 3rd December 1999); Opinion 3/2000 on the EU/U.S dialogue concerning the 'Safe Harbor' arrangement, 5019/00/EN/FINAL, WP 31, (adopted on 16th March 2000); Opinion 4/2000 on the level of protection provided by 'Safe Harbor Principles', CA07/434/00/EN, WP 32, (adopted on 16th May 2000); Opinion 6/2002 on Transmission of Passenger Manifest Information and other Data from Airlines to the United States, 11647/02/EN, WP 66, (adopted on 24th October 2002); Opinion 8/2004 on the Information for Passengers concerning the Transfer of PNR Data on Flights between the European Union and the United States of America, 11733/04/EN, WP 97, (adopted on 30th September 2004); Opinion 5/2006 on the Ruling by the European Court of Justice of 30 May 2006 in Joined cases C-317/04 and C-318/04 on the Transmission of Passenger Name Records to the United States, 1015/06/EN, WP 122, (adopted on 14th June 2006); Opinion 7/2006 on the Ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the Transmission of Passenger Name Records to the United States and the urgent Need for a new Agreement, 1612/06/EN, WP 124, (adopted on 27th September 2006); Opinion 5/2007 on the Follow-up Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record(PNR) Data by Air Carriers to the United States Department of Homeland Security concluded in July 2007, 01646/07/EN, WP 138, (adopted on 17th August 2007); Joint Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record(PNR) for Law Enforcement Purposes, presented by the commission on 6 November 2007, 02422/07/EN, Art 29 WP ref: WP 145, WPPJ ref: 01/07, (adopted on 5th December 2007).

[1068] See U.S Department of Commerce, Export Portal 'Helping U.S Companies Export', http://export.gov/safeharbor/eu/eg_main_018493.asp last visited 21/01/2012.

[1069] Ibid.

[1070] Ibid; see also Hubbard, note 1049.

(b) Safe Harbor Principles

The Safe Harbor Framework policy has seven principles.[1071] In addition, it is accompanied by fifteen 'Frequently Asked Questions (FAQs)' and their corresponding answers.[1072] The latter provide guidance on interpretation and implementation of the entire framework policy.

- **Notice**

Notice reflects the purpose specification principle found in most data protection instruments. Essentially it requires that U.S firms receiving personal data from the European Union must inform the individuals about the purpose for which such information was collected, its uses, including further transfer to third parties. Also 'notice' requires that the details about the firm collecting information and how it may be contacted be made available to the individuals. More details required to be availed to individuals include information about inquiries, complaints and directions on use limitation. In case of change of original purpose or transferring of individuals' to third parties, the notice must be communicated before.

- **Choice**

Choice requires organisations processing information to give data subjects options to choose or opt out whenever the controller intends to disclose the information to third parties or change use from the original purpose. The choice must be clearly brought into the attention of the data subject, and should not be costly in terms of the means to exercise it. Stringent rules apply in case of sensitive personal information. Here affirmative or explicit (opt in) option must be given if there are plans to disclose such information to third parties or change of use is anticipated.

- **Onward Transfer**

This principle restricts transfer by the receiving organisation of personal information from Europe to third parties except where they meet the adequate data protection. Compliance to the SH meets the adequacy test. Also, transfer may be made to any other third party in a country where the European Commission has made a finding of adequacy protection. Contractual

[1071] Safe Harbor Policy Principles, note 1037, supra.
[1072] Ibid.

clauses can also be used to transfer data to third party in a country which has not been found to provide adequate level of data protection by the European Commission. If the receiving third party does not process data in accordance with the required standards, the sending firm is not held responsible as long as it was not aware of inappropriate processing of such information. Yet it is duty bound to stop the transfer.

- **Security**

This principle puts under obligation firms which process personal information to take reasonable steps to secure such information against loss, misuse, unauthorised access, disclosure, alteration and destruction.

- **Data integrity**

Data integrity requires collection of only relevant information to the purpose for which such information is sought to be collected. This principle puts obligation on firms to ensure that data under their control is reliable for its intended use, accurate, complete and current.

- **Access**

Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. The 'access' principle depends upon the principle of 'notice' in that the data subject must be aware of who holds his/her personal information and how to contact him/her before any exercise of the rights of correction, amendment or deletion.

- **Enforcement**

In order to ensure compliance with the SH principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to

adhere to the SH principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and SH benefits will no longer be assured.

(c) Adequacy and Subsequent Evaluation and Monitoring

In 2000 the European Commission issued its decision declaring that the Safe Harbor Framework meets the adequacy test of data protection set out in Directive 95/46/EC.[1073] The Commission's decision was in sharp contrast with the opinion of the Article 29 Working Party which throughout opined that the U.S approach to data protection would not provide such adequate protection.[1074] At least this was a rare opportunity the Article 29 Working Party's negative opinion had been direct and publicized, especially for world's most superpower like the United States. More probably, the Working Party's opinion was based on the overall U.S tradition and approach towards privacy protection i.e. self-regulation of the private sector. This view can further be understood in another context where the Article 29 Working Party issued a negative opinion on the U.S Passenger Name Records (PNR) for an arrangement which U.S authorities required transmission of airline passenger manifests of all people travelling from Europe to U.S immediately after the aircrafts leave European airports.[1075] Yet, the Commission proceeded to issue an adequacy label to the arrangement.[1076] Subsequently, the European Court of Justice nullified the agreement between the European Community and the United States of America on PNR,[1077] though based on the competency of the matters transacted, it is still doubtful if on merit, the ECJ would still hold that such an agreement does not infringe the provisions of Directive 95/46/EC. It is interesting to note that a renewal of the earlier agreement after adjustments has remained unsigned to date since 2007, presumably reflecting the unsatisfactory level of protection of privacy in the U.S.[1078]

[1073] Commission Decision, C (2000), 2441, note 865, supra; see also, Greenleaf, G., 'Safe Harbor's Low Benchmark for "adequacy": EU sells out Privacy for US$', Privacy Law & Policy Reporter, 2000, Vol. 7, No.3, pp.45-49.
[1074] Article 29 Data Protection Working Party, note 1067, supra.
[1075] Ibid.
[1076] Commission Decision, C (2004), 1914, note 865, supra.
[1077] European Parliament v. Council of the European Union and Commission of the European Communities, Joined Cases C-317/04 and 318/04 (judgement delivered on 30 May 2006).
[1078] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), O.J.L204/16 of 4.08.2007, approved the signing of the Agreement but to date it has never been signed.

Two points can be made regarding the positive adequacy finding for the SH and certainly PNR. First, the finding reflects the economic mighty of U.S globally and its large share in the EU-U.S trade relationship. Second, the two sides of the Atlantic have 'relatively comparable bargaining powers'[1079] in which case it is difficult for one of them to dictate terms on the other. This further suggests that where the relative powers of the clashing parties are comparable, a more co-operative form of policy co-ordination can result.[1080] Hence only a compromise is necessary. It can safely be submitted that the adequacy finding on SH and PNR were no more than 'adequacy by affirmative action' or 'adequacy without qualification' which EU may not be prepared to forge another SH by any other non-EU/EEA country.

However, despite the adequacy finding label of the SH by the Commission in 2000, subsequent evaluation and monitoring has revealed compliant deficits. Some of these deficits are inherent in the SH Framework compromises themselves while others are external, largely arising from the failure by the U.S firms and authorities to abide to the SH principles. For instance, the scope of the SH is limited to electronic data and does not apply to personal information in manual filing system.[1081] This means privacy violations in the manual filing system are left outside the ambit of the SH policy. Also, the SH Framework applies only to a limited number of firms falling under the enforcement jurisdiction of the U.S Department of Transportation or under the Federal Trade commission.[1082] All other business sectors (e.g. health care and banking) are not eligible.[1083] Moreover, the policy framework is self-certifying. Companies choose whether or not to enter the SH. This undermines the whole rationale for which the SH was adopted. Additionally, the timing of the protection is based on the date that the company certifies its compliance to both the U.S Department of Commerce and public announcement of its entry into the program.[1084] Interestingly, the Department of Commerce does not further verify the information in the self-certification form. Yet, all data flows after public announcement and self-certification filing are protected by the Safe Harbor provision. Consequently, the Commission waives the requirement for prior authorization by a data protection body for transfers to the U.S or requires prompt or

[1079] Long and Quek, note 1044, supra.
[1080] Ibid, p.340; see also, Shaffer, G., 'Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements', Columbia Journal of European Law, 2002, Vol.9, No.1, pp.29-78; Roos, M., 'Definition of the Problem: The Impossibility of Compliance with both European Union and United States', Transnational Law & Contemporary Problems, 2005, Vol.14, No.3, pp.1137-1162; May, B.E *et al.*, 'The Differences of Regulatory Models and Internet Regulation in the European Union and the United States', Information & Communications Technology Law, 2004, Vol.13, No.3, pp.259-272.
[1081] Hubbard, p.6, note 1049, supra.
[1082] Ibid, p.5.
[1083] Ibid.
[1084] Ibid, note 1081, supra.

automatic approval of the transfer.[1085] Also important to note, the SH includes three sets of explicit exceptions where compliance with its provisions may be limited: for reasons such as national security, public interest, or law enforcement requirements; by statute, government regulation or judicial determination that creates conflicting obligations or explicit authorizations, provided that the derogations are narrowly tailored; or if the Directive or member state law allows exceptions or derogations. These sets of exceptions are quite extensive and practically render the protection afforded by the policy severely limited.

The above limitations in the SH Framework and those manifesting out of its implementation are partly reflected in the subsequent reports and opinions by the European Commission and Article 29 Working Party regarding the operation of SH.[1086] Although those reports and opinions suggest that the SH may be subjected into review it is unlikely that this will happen in the near future. The pain and difficulties EU and U.S went through in negotiating the SH are the factors that may partly operate against any soonest review process. Yet the adoption of the General Data Protection Regulation by EU, which though may not significantly alter the basic data protection principles under the Directive, may be used by EU to pull the United States into negotiating table. However, this may take sometime especially after the Regulation has become operational and possibly produced some negative effects in the operation of the SH. On the side of U.S, some efforts are being made to regulate processing of personal data like proposing the Commercial Privacy Bill of Rights Act of 2011;[1087] nevertheless these efforts are seen as mostly 'for show'[1088] possibly to tell their EU counterpart that they are taking privacy seriously. One of the reason for this view is the over dominance of incorporation of 'self-regulation' and 'multiple safe harbors' in the proposed Bill. In her recent speech towards the end of the year 2011, Viviane Reding (the Vice-President of the European Commission, EU Justice Commissioner) openly criticized the U.S Commercial Privacy Bill of Rights that the U.S 'self-regulation' may not be sufficient to achieve full interoperability between the EU and U.S.[1089] This comment clearly indicates that the two sides of the Atlantic are still far apart in terms of data protection policies and it may be difficult to completely reconcile their approaches. It has to be seen as events

[1085] Ibid.

[1086] Article 29 Data Protection Working Party., 'Working Document on Functioning of the Safe Harbor Agreement', 11194/02/EN, WP 62, (adopted on 2nd July 2002); European Commission., 'Commission Staff Working Document on the Implementation of Commission Decision 520/2000/EC on the adequacy protection of personal data provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the U.S Department of Commerce', SEC82004) 1323, Brussels, 20.10.2004.

[1087] A Bill to establish a regulatory framework for the comprehensive protection of personal data for individuals under aegis of the Federal Trade Commission, and for other purposes, April, 12, 2011.

[1088] Gellman and Dixon, p.10, note 891, supra.

[1089] Reding, V., 'The Future of Data Protection and Transatlantic Cooperation', Speech at the 2nd Annual European Data Protection and Privacy Conference (SPEECH/11/851), Brussels, 6 December 2011, pp. 1-4, at p.4.

unfold-especially the need for more commercial relationship between EU and the United States, development of modern technologies particularly 'cloud computing', enhancement of the EU data protection policies and laws in response to the need for further protection of personal data, increased security, etc if the EU and U.S policies on privacy protection will finally converge.

3.3.3 Asia-Pacific Region

The Asia-Pacific Economic Cooperation (APEC) is an economic forum of twenty one member economies drawn from Asia, North America, South America and Australia.[1090] The forum was established in 1989 with three main goals: to develop and strengthen the multilateral trading system; to increase the interdependence and prosperity of member economies and to promote sustainable economic growth.[1091] The APEC has more than 2.7 billion people and represents approximately 54 percent of the world real GDP and 44 percent of world trade.[1092] In contrast to most world's regional groupings, APEC operates on the basis of open dialogue and respect for views of all participants.[1093] All economies have equal say and decision-making is reached by consensus.[1094] There are no binding commitments; compliance is achieved through discussion and mutual support in the form of economic and technical cooperation.[1095] These features have far reaching implications to almost every aspect of the APEC's operations.

In November 2004 APEC adopted the APEC Privacy Framework- through a process that had taken the forum two years to complete. Given the diversities of economies, social and political levels of developments as well as different cultural backgrounds, one would have expected the negotiations of the APEC Privacy Framework to have taken a longer period. Yet, that was not the case partly because the Framework is non-binding and compliance is voluntary. Moreover, it may be viewed that the adoption of the APEC Privacy Framework was geared towards counter-balancing the bureaucratic burden and 'adequacy' requirements of European Union's Directive 95/46/EC rather than creating strong commitment to protection of personal data hence no

[1090] Currently APEC has the following members: Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, South Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru Philippines, Russia, Singapore, Taiwan, Thailand, USA, and Vietnam. These members are commonly described as 'economies' because the APEC cooperative process is predominantly concerned with trade and economic issues, with members engaging with one another as economic entities; see APEC Website, http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx last visited 26/01/2012.

[1091] APEC., 'APEC at Glance 2011', http://publications.apec.org/publication-detail.php?pub_id=1077 last visited 26/01/2012.

[1092] Ibid.

[1093] Ibid.

[1094] Ibid.

[1095] Ibid.

serious privacy concerns were driving force behind the Framework.[1096] However this attempt which was ideologically synchronized by Australia and the U.S.A to form an 'APEC block' that either explicitly rejected or ignored any European privacy standards has not yet succeeded in fashioning APEC into any such thing.[1097] Also important to note, the process leading to the adoption of APEC Privacy Framework did not take long perhaps because APEC reproduced, without any serious discussion, most of the privacy principles found in the *OECD Guidelines* with only minor differences which often lead to provision of weaker standards. This reproduction has quite often received negative commentaries.[1098] The chief criticism is the fact that the *OECD Guidelines* upon which the APEC Privacy Framework is based were twenty years old and had little, if any, reference to modern technologies at the time the Framework was adopted. Hence reliance on them would not in any case result into a regulation that has taken into account possibilities of privacy infringements committed using modern technologies.

Another point that needs to be made clear with respect to the process leading to the adoption of the APEC Privacy Framework in 2004 is that, the latter was still a work-in-progress. In 2004, when adopted, the Framework incorporated four major parts: Preamble (Part I); Scope (Part II); APEC Information Privacy Principles and the Commentary (Part III) and Implementation (Part IV). The latter part (i.e. Part IV) was incomplete as it only contained 'Guidance for Domestic Implementation' under Section A. Section B on cross-border rules was still missing. This section was completed in September 2005 following the incorporation of 'Guidance for International Implementation'.

[1096] For an opposite view see e.g., Tan, J.G., 'What effect is the APEC Privacy Framework likely to have in the struggle between the EU and APEC states to establish global standards for data protection?', A Tutorial Paper presented at the Norwegian Research Centre for Computers and Law (NRCCL), Spring, 2006, pp.1-9, at p.2, who argues that the emergence of the APEC Privacy Framework should not be viewed as a struggle between EU and APEC states. Rather the APEC Framework paves the way for further dialogue on the emergence of a global standard for data protection.

[1097] Ford, P., 'Implementing the Data Protection Directive - An Outside Perspective', Privacy Law & Policy Reporter, 2003, Vol. 9, pp. 141-149 cited in Greenleaf, p.17, note 560, supra.

[1098] See e.g., Greenleaf, G., 'Australia's APEC Privacy Initiative: The Pros and Cons of "OECD Lite"' Privacy Law & Policy Reporter, 2003, Vol.10, pp. 1-6; Greenleaf, G., 'APEC Privacy Principles Version 2 - Not quite so Lite, and NZ wants OECD full strength', Privacy Law & Policy Reporter, 2003, Vol. 10, pp. 45-49; Greenleaf, G., 'APEC Privacy Principles: More Lite with every version', Privacy Law & Policy Reporter, 2003, Vol.10, pp. 105-111; Greenleaf, note 695, supra; Greenleaf, G., 'Criticisms of the APEC Privacy Principles (Version 9), and recommendations for improvements', Working Paper, March 2004, http://www2.austlii.edu.au/%7Egraham/publications/2004/APEC_V9_critique/APEC_V9_critique.html last visited 29/01/2012; Greenleaf G., 'APEC's Privacy Framework: A new low standard', Privacy Law & Policy Reporter, 2005, Vol. 11, pp.121-124; IT Law Group., 'Neither a Floor nor a Ceiling: the APEC Privacy Framework fails to harmonize the Privacy Regime in the Asia Pacific Region', http://www.itlawgroup.com/resources/articles/142-marketing-and-sales.html last visited 29/01/2012; Munir, A.B., 'Implementation of the APEC Privacy Framework in National Regulation', Paper Presentation during Workshop on International Data Sharing and Biometric Identification, Royal Plaza Hotel, Singapore, 2-3 July 2009, http://www.hideproject.org/downloads/ws-singapore/HIDE_WS-Annex_IIId-Presentation_Abu_Bakar_Bin_Munir-20090702.pdf last visited 29/01/2012.

Generally, the objectives served by the APEC Privacy Framework and the philosophy behind it are rooted in the APEC's broader objectives for its establishment. The Framework states in its preamble that its broad aims are to promote electronic commerce and ensure free flow of information within the APEC economies. Also it sets out as its main agenda to protect privacy. Nevertheless, economic concerns are clearly dominant.[1099] The Framework scarcely, if at all, alludes to privacy safeguards as fundamental rights.[1100] Undoubtedly, because of this omission which is attributed by different histories and experiences between the West and Asia-Pacific countries; the entire Framework fails to measure up the European instruments on protection of privacy, more particularly the Directive 95/46/EC which treats and protects privacy as a fundamental right.

The scope of the APEC Framework is similar to that of the *OECD Guidelines* and the Directive 95/46/EC. The former extends its application to processing of personal data of natural persons, in both public and private sectors with regard to automated or manual data files.[1101] It excludes processing of family or household activities such as keeping address books and phone lists or preparing family newsletters.[1102] Also excluded from the application of the Framework are matters of public available information and those touching national security, public safety and public policy.[1103]

Unlike the *OECD Guidelines,* the APEC Framework has nine information privacy principles. The latter has left out the principle of 'openness' from the set of eight principles found in the *OECD Guidelines*. Yet, it added the principles of 'preventing harm' and 'notice'. Similarly the scope and formulations of these principles differ significantly in some places from the OECD. The nine APEC information privacy principles are:-

- **Preventing Harm**

The preventing harm principle seeks to protect individuals against wrongful collection or misuse of their personal data. Under this principle privacy protections are required to be designed to achieve these aims. Also, the principle requires adoption of the appropriate remedies which are proportionate to the likelihood and severity of the risk of harm.

[1099] Bygrave, p.44, note 503, supra.
[1100] Ibid.
[1101] APEC Privacy Framework, Paras 9 and 10.
[1102] Ibid, Para 10.
[1103] Ibid, Paras 11, 13 and Part III.

- **Notice**

This principle imposes an obligation on the party of the data controller to notify data subjects a range of information. The latter includes what information is collected and for what purposes it was collected; persons/ organizations to whom personal information might be disclosed; identity and location of the controller; choices and means the controller offers individuals for limiting use and disclosure as well as accessing and correcting their information. Furthermore, this principle places additional obligation on the controller to take reasonably practical steps to provide notice either before or at the time of collection, or as soon after as is practicable.

- **Collection Limitations**

The collection limitation principle requires that only relevant information that is related to the specified purpose should be collected. Also, it places the obligation on controllers to obtain personal information from data subjects by lawful and fair means. Where it is appropriate the collection must be commenced with notice to, or consent of, the individual concerned.

- **Uses of Personal Information**

This principle imposes limitations on the use of personal information only to fulfill the purposes of collection and other compatible related purposes.

- **Choice**

The choice principle requires that where it is appropriate individuals should be provided with affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.

- **Integrity of Personal Information**

The principle of integrity of personal information states that personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

- **Security Safeguards**

This principle places obligation on data controllers to apply appropriate safeguards that will protect personal information against risks such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuse. It also requires that such safeguards should be proportional to the likelihood and severity of the harm threatened the sensitivity of the information, and the extent in which it is held, and should be subject to periodic review and assessment.

- **Access and Correction**

Individuals should be afforded rights to access to their personal data and challenge its accuracy, and as appropriate request rectification, completeness, amendment or deletion of such personal information.

- **Accountability**

The accountability principle requires that data controllers comply with measures that give effect to the principles under the Framework. In event of data transfers by data controllers whether domestically or internationally, they must ensure those recipients of such data protect the received personal information in a manner consistent with these principles.

Domestically, the implementation of the APEC Privacy Framework is left at discretion and flexibilities of the member economies. Member economies may opt to protect privacy through legislation, administrative means, industry self-regulations or a combination of these methods.[1104] The Framework also requires its implementation be flexible in such manner as to accommodate various methods including central authorities, multi-agency enforcement bodies, a network of designated industry bodies, or a combination of these methods.[1105] Similarly, the Framework takes into account that some member states may have already adopted domestic privacy protection prior to the Framework. In such cases member economies are urged to take all reasonable steps to identify and remove unnecessary barriers to information flows and avoid the

[1104] APEC Privacy Framework, Para 31.
[1105] Ibid.

creation of any such barriers.[1106] The Framework incorporates requirements for educating and publicizing domestic privacy protections;[1107] cooperation between private and public sectors;[1108] provision of appropriate remedies in situations where privacy protections are violated;[1109] and mechanisms for reporting domestic implementation of the APEC Privacy Framework through completion of and periodic updates to the Individual Action Plan (IAP) on information privacy.[1110]

International implementation of the APEC Privacy Framework envisages information sharing among member economies;[1111] cross-border cooperation in investigation and enforcement;[1112] and cooperative development of cross-border privacy rules.[1113] The Framework does not contain any specific rules that regulate international transfers of personal data from the APEC region to non-APEC member economies (i.e. third countries). It is also important to note that in order to facilitate the goals of the APEC Privacy Framework and more particularly to ensure smooth cross-border flows of personal information, the APEC Ministers endorsed the establishment of the APEC Data Protection Pathfinder in 2007 to carry out a number of projects.[1114] Recently the APEC Ministers, through the Pathfinder's roles, have adopted and endorsed Cross-Border Privacy Rules (CBPR) similar but slightly different from the EU's Binding Corporate Rules(BCR) scheme. [1115]

In relative terms, the APEC Privacy Framework has received many criticisms. Most of them have been raised by Professor Graham Greenleaf, who perhaps, more than any other commentators in the field, has closely followed the development of the Framework since its preparation, inception to practice and published extensively on APEC Framework. In summary these criticisms are based on the broad scope of the Framework's information privacy principles; vagueness and imprecise definitions; ignoring regional experience; incorporation of potentially retrograde new principles; ignoring EU compatibility; adopting and further weakening OECD

[1106] Ibid, Para 30.
[1107] Ibid, Paras 35 and 36.
[1108] Ibid, Para 37.
[1109] Ibid, Para 38.
[1110] Ibid, Para 39.
[1111] Ibid, Paras 42 and 43.
[1112] Ibid, Paras 44 and 45.
[1113] Ibid, Paras 46,47 and 48.
[1114] APEC Data Privacy Pathfinder; http://apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx last visited 30/01/2012.
[1115] For shorter analysis of these rules see e.g., Stewart, B., 'Towards Global Solutions: APEC Ministers endorse Cross-Border Privacy Rules Scheme', Privacy Laws & Business International Report, 2011, No.114, pp.14-15.

principles.[1116] With regard to implementation, many commentators including Greenleaf fault the APEC Privacy Framework for its failure to forbid data exports to countries without APEC-compliant laws or explicitly allow restrictions on data exports to countries without APEC-compliant laws or at least require data exports to be allowed to countries that have APEC-compliant laws.[1117] Accordingly, Greenleaf argues that the APEC Privacy Framework is extremely non-prescriptive in relation to data exports, consistent with its general non-prescriptive nature.[1118] His overall assessment of the impact of the Framework in the APEC region is that the former has been too weak to stimulate privacy regulation.[1119] Greenleaf has rated the European Directive 95/46/EC as the most influential in the APEC region.[1120] Its influence has been felt in a number of jurisdictions such as India, Macao, Korea, Malaysia, Philippines, China and New Zealand.[1121] The latter is about to be confirmed by EU as providing 'adequate' level of data protection. Next to the Directive, the author rates the *OECD Guidelines* whose influence has already been seen in Australia, New Zealand, Hong Kong, Korea, Japan and Indonesia.[1122] On the other end of the spectrum, there are authors who have been uncritical to the APEC Framework. These have argued that while at first glance there appears to be deficiencies in the APEC Framework, its value should not be overlooked.[1123] The APEC Framework represents a consensus between countries who come from different legal systems, different values and are at different stages of enacting their privacy legislation.[1124] These commentators also argue that the Framework involves countries who have not been previously party to any international agreement regarding data protection and privacy but who are likely to be players in the world economy in the near future.[1125] Yet, there are authors who have attempted to take a balanced position between the critical and uncritical commentators. For example, Waters argues that the APEC Privacy Framework is neither a particular good alternative model for balancing privacy protection and free flow of information nor a major

[1116] Greenleaf, pp.8-21, note 560, supra; see also, Kennedy, G *et al.*, 'Data Protection in the Asia-Pacific Region', Computer Law & Security Review, 2009, Vol.25, No.1, pp.59-68.
[1117] Greenleaf, p.16, note 560; see also, Bygrave, note 1099, supra.
[1118] Greenleaf, note 117, supra.
[1119] Greenleaf, p.13, note 695, supra.
[1120] Ibid.
[1121] Ibid.
[1122] Ibid.
[1123] Tan, p.8, note 1096, supra; see also Tan, J.G., 'A Comparative Study of the APEC Privacy Framework-A New Voice in the Data Protection Dialogue?', Asian Journal of Comparative Law, 2008, Vol.3, No.1, pp.1-44, at p.31; Bulford, C., 'Between East and West: The APEC Privacy Framework and the Balance of International Data Flows', I/S: A Journal of Law and Policy for the Information Society, 2008, Vol.3, No.3, pp.705-722, at pp.719-722.
[1124] Ibid.
[1125] Ibid.

threat to existing levels of privacy protection.[1126] For Waters, the differences between the APEC Framework and the other international privacy instruments are not as great as has been suggested, while the deficiencies and obstacles to effective implementation are very similar.[1127]

The conflicting opinions over the efficacy of the APEC Privacy Framework reveal one major problem: the lack of an 'ideal standard' which in any case is difficult to set across different cultures, economic and political systems. As it can be noted, from European regulatory point of view which is rooted in human rights sentiments, the APEC Framework provides weak standard while from the APEC member economies which place commerce at the forefront and privacy as just as secondary issue the Framework offers a more flexible and perfect scheme. This explains further the problem of achieving global policies and regulatory frameworks for protection of privacy and personal data. However through dialogue at the global level policies and frameworks which set common minimum standards can be forged. Yet, as many commentators opine, the adoption of such policies and frameworks is a process which is still far away.

3.3.4 Organization of the Islamic Cooperation

The Cairo Declaration on Human Rights in Islam [1128](CDHRI or Islamic Charter) is the human rights instrument for the Organisation of the Islamic Cooperation (OIC) formerly known as the Organisation of the Islamic Conference (OIC). The latter was established on 25 September 1969 with the objective of safeguarding and promoting the interests of the Muslim world in diverse number of issues: fraternity and solidarity; common interests and support of legitimate causes; self-determination; sovereignty and territorial integrity; participation in the global decision-making processes; inter-state relations; support of the rights of peoples as stipulated in the United Nations and international law; Palestinian self-determination; intra-Islamic economic and trade cooperation; human development and economic well-being; Islamic teachings and values; defending true image of Islam; enhancement and development of science and technology; protection of family; safeguarding rights of Muslim communities and minorities in non-member states; common interests in international fora; combating terrorism; humanitarian emergences;

[1126] Waters, N., 'The APEC Asia-Pacific Privacy Initiative-A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation?', SCRIPTed, 2009, Vol.6, No.1, pp.74-89, at p.88; see also Connolly, C., 'Asia-Pacific Region at the Privacy Crossroads', World Data Protection Report, 2008, Vol.8, No.9, pp.8-16.
[1127] Waters, note 1126, supra.
[1128] U.N. Doc. A/45/421/5/21797, p.199, (adopted on 5th August 1990).

and cooperation in social, cultural and information.[1129] OIC is the second largest inter-governmental organization after the United Nations.[1130] At present, it has fifty seven member states scattering in four world's continents.[1131] Some member states are secular while others are non-secular and have declared Islam as the state religion with *sharia* as the supreme law superior even to the states' constitutions.[1132]

CDHRI guarantees the right to privacy in Art 18(b) as follows: 'everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The state shall protect him from arbitrary interference.'

Although the above provision seeks to protect privacy just like the other international codes, its formulation and the entire environment in which it operates (more specifically in Islamic states) has sparked much debates critical and uncritical and those sought a compromise. These debates have centered around the compatibility of Islamic practices and the legal tradition on *sharia* with the human rights and values which originated from the Western European cultures.[1133] More debates have recently been raised with regard to the ability of data protection legislation to effectively secure individuals' rights to privacy in Islamic states.[1134]

3.3.5 League of Arab States

The Arab Charter of Human Rights 2004[1135](ACHR) is the main human right instrument for the League of Arab States (informally known as the Arab League). The latter was founded on 22

[1129] OIC, Charter of the Organisation of the Islamic Conference 2008(replacing the original Charter registered the United Nations on 1st February 1974), Art 1.
[1130] OIC, Website, http://www.oic-oci.org/page_detail.asp?p_id=52 last visited 31/01/2012.
[1131] Azerbaijan, Jordan, Afghanistan, Albania, United Arab Emirates, Indonesia, Uzbekistan, Uganda, Iran, Pakistan, Bahrain, Brunei-Darussalam, Bangladesh, Benin, Burkina Faso, Tajikistan, Turkey, Turkmenistan, Chad, Togo, Tunisia, Algeria, Djibouti, Saudi Arabia, Senegal, Sudan, Syria, Suriname, Somalia, Sierra Leone, Iraq, Oman, Gabon, Gambia, Guyana, Guinea, Guinea-Bissau, Palestine, Comoro, Kyrgyz, Qatar, Kazakhstan, Cameroon, Ivory Coast, Kuwait, Lebanon, Libya, Maldives, Mali, Malaysia, Egypt, Morocco, Mauritania, Mozambique, Niger, Nigeria, and Yemen; see OIC, Website, http://www.oic-oci.org/member_states.asp last visited 31/1/2012.
[1132] See e.g. the North African Arab states: Tunisia, Morocco, Algeria, Libya and Egypt. Note that, this is not the exhaustive catalogue of such OIC's states which are Islamic and the Shari' ah as their supreme source of law.
[1133] See e.g., Qureshi, Ezzat, Talbi, Ahmad and McCrea, note 197, supra; Cannataci, pp.5-6, note 29, supra; Arzt, D.E., 'The Application of International Human Rights Law in Islamic States', Human rights Quarterly, 1990, Vol.12, No.2, pp.202-230.
[1134] See e.g., Caurana and Canataci, note 152, supra; Azmi, note 158, supra; Hayat, note 161, supra; Kusamotu, note 164, supra and Bonnici, note 167, supra.
[1135] The Arab Charter on Human Rights was initially adopted in 1994 but it did not come into force because of criticisms which only saw one ratification (Iraq) out of the 22 members hence insufficiency number of ratification. The new version (Arab Charter on Human Rights 2004) was adopted in 2004 and came into force 15th March 2008.

March 1945 earlier than the United Nations.[1136] The Arab League has twenty two members including Syria which was suspended on 16 November 2011.[1137] All of the states in the Arab League are also members to the OIC. The main objectives for which the Arab League was establish are to strengthen ties among its members, coordinate their policies and promote their common interests.[1138]

Article 21 of the Arab Charter on Human Rights protects privacy. This provision states that no one shall be subjected to arbitrary or unlawful interference with regard to his privacy, family, home or correspondence, nor to unlawful attacks on his honour or his reputation. To safeguard this right, the Charter provides further that everyone has the right to the protection of the law against such interference or attacks.

Undoubtedly, Article 21 of the Arab Charter on Human Rights reproduces verbatim Article 12 of the Universal Declaration of Human Rights 1948 which secures the right to privacy. It is widely viewed by commentators that this reproduction has been necessitated by an attempt to avoid the potential criticisms similar to those waged against the Cairo Declaration on Human Rights in Islam.[1139] Yet, privacy is a right in the ACHR. Its effective protection depends on the wider environment in which it operates and also on other provisions of protection of human rights. As pointed out, there are difficulties of the operation of human rights in the Arab League. Part and parcel of them are the fact that majority of the member states practice *sharia* law, Islamic religion and Arab culture-all of them complicating the environment for the operation of the right to privacy.[1140]

3.5 Conclusion

The review of privacy and data protection codes at the international plane depicts some common and divergent trends. First, almost all international human rights catalogues contain the right to privacy. Although such a right is broadly framed hence cannot secure protection of personal data

[1136] Pact of the League of the Arab States (22nd March 1945).
[1137] Other members of the Arab League are Algeria, Bahrain, Comoros, Djibouti, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Mauritania, Morocco, Oman, State of Palestine, Qatar, Saudi Arabia, Somalia, Sudan, Tunisia, United Arab Emirates and Yemen, see Website of the League of Arab States.
[1138] See Art 1 of the Alexandria Protocol (7th October 1944) signed by the heads of governments of Egypt, Trans-Jordan, Syria, Iraq and Lebanon (among the six founders of the Arab League); see also Art 2 of the Pact of the League of the Arab States.
[1139] Cannataci, p.6, note 29, supra.
[1140] See e.g., Rishmawi, M., 'The Revised Arab Charter on Human Rights: A Step Forward?', Human Rights Law Review, 2005, Vol.5, No.2, pp.361-376; Rishmawi, M., 'The Arab Charter on Human Rights and the League of Arab States: An Update', Human Rights Law Review, 2010, vol.10, No.1, pp.169-178.

as such, it has provided strong normative force for the existence of data protection laws. Second, there is no single approach to protection of personal data. In Europe a comprehensive approach with a set of data protection principles and centralized supervisory authorities has been mostly favored. Yet, in some other places more particularly the United States, industry self-regulation is mostly preferred. In the Asia Pacific region, the approach is too pragmatic. In the last two cases 'market' rather than human rights sentiments are the driving forces behind such approaches. The OIC and the Arab League have not yet developed concrete policy and regulatory framework regarding the protection of personal data. Third, since countries have different regional and international commitments there are cross-cutting effects of the data protection policies and frameworks, as such, although some countries in particular regions are dominantly relying on 'market' to self-regulate personal data, they have not escaped the influence of regions which rely on comprehensive regulation of personal data. Yet, this effect has mainly not been in reverse. Fourth, of all international codes of data protection, the EU Directive 95/46/EC has been the most influential catalyst for adoption of data privacy legislation in Europe and to non-European countries. Part and parcel of this influence is generated by the exterritorial reach of the Directive through the requirement of limitation of transfer of personal data from EU/EEA to non-EU/EEA countries (i.e. third countries) where such countries do not provide 'adequate' level of data protection similar to the Directive itself. This requirement which has affected the relationship between Europe and the third countries particularly in trade has exerted enormous pressure on the latter to adopt comprehensive data privacy law in the European style in order to sustain trade relationships. Sometimes 'adequacy' requirement has compelled Europe to make a number of compromises. In order to ensure third countries have complied with the required 'adequacy' level of data protection, Europe has institutionalized the accreditation process. Through this procedure third countries 'voluntarily' make application to European institutions for accreditation. The latter assess the level of data protection using a set of criteria which are transparently known to third countries. Yet, extraneous criteria only known to European institutions are frequently invoked. This has rendered the whole process not only cumbersome but also unpredictable in its outcomes.

Based on the above trends, and in particular, the over dominance of the European Directive 95/46/EC worldly, this study selects it as the policy and regulatory framework informing subsequent discussions and analyses. There are two more reasons which have influenced this choice. Recently (2012), the European Union is carrying out legislative process for adopting the General Regulation of Data Protection to enhance the effects of the Directive's 'adequacy'

requirements. As such the influence of the European law to non-European countries will be accelerated and is likely to have far reaching impacts. Second, the emerging legislative trend of data protection in Africa reveals that the same has closely followed the EU-style under Directive 95/46/EC. Moreover, some of these jurisdictions have gone a step further to apply and seek accreditation with the European Union's institutions (see chapters 4, 5, 6 and 7).

4. Privacy and Data Protection in Africa

4.1 Introduction

This chapter serves as a general introduction to chapters 5, 6 and 7 which are case studies of the present research. It canvasses a set of three interrelated issues. The first set generally surveys the socio-economic and political context of the African continent in order to lay down foundation for subsequent discussion. The rationale for undertaking this general survey is simply that privacy is not entirely independent from economic, political and technological forces. To accomplish this, a historical perspective of the changing epochs is engaged. The second set of issues covers African societal norms, particularly the norm of privacy. Understandably, it is risk to undertake a generalised approach on the norm of privacy in this second set because of lack of homogeneous socio-economic, political and technological perspectives across Africa. Yet, some minimum common traits and characteristics are still possible to analyse. The third and final set of issues addressed in this chapter relates to the regulation of privacy and personal data. Both policy and regulatory frameworks are broadly covered. The latter are considered at regional, sub-regional and national levels. Yet, specific and detailed discussions on national policies and regulatory frameworks are kept at minimum. These discussions are reserved for detailed analyses in chapters 5, 6 and 7.

4.2 Political and Economic Context

Africa is the world's second largest continent in terms of size and population after Asia. It is made up of fifty four independent states.[1141] Its total area covers about 11,677,239 square miles. Africa's population as recorded by the World Bank in 2010 was 853.6 million (excluding North Africa).[1142] In the same year the United Nations recoded Africa's population at 1,022,234,000 (over 1 billion) with an inclusion of North Africa.[1143] The average growth rate of this population is approximately 2.5 per annum.[1144] However its settlement population pattern is such that by 2011 more Africans were still living in rural areas than in urban centers. While in the former case

[1141] See a complete list of these countries in notes 194 and 195 supra.
[1142] World Bank's Website, http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/AFRICAEXT/EXTPUBREP/EXTSTATINAFR/0,,menuPK:824057~pagePK:64168427~piPK:64168435~theSitePK:824043,00.html last visited 3/02/2012.
[1143] See United Nations' World Population Prospects, the 2010 Revision http://en.wikipedia.org/wiki/List_of_continents_by_population last visited 3/02/2012.
[1144] World Bank, note 1142, supra.

the population was 60% in the latter was only 40%.[1145] Yet the urban population growth rate currently stands at 3.4% a year.[1146] Accordingly it is estimated that 60% of African people will be living in cities by 2050.[1147] At least 14 African countries are expected to be at least 80% urbanized by 2050.[1148] Although the reasons for this growth are a mixture of factors, the rural to urban migration plays a significant role. Lack of employment, access to services and perceived opportunities of cities are widely considered to encourage people to migrate from rural areas to cities.[1149]

Politically, African states especially those found in south of the Sahara have presidential system of government where the president is both the head of the state and head of government. Politics in these countries is practiced through liberal multi-party political system although not without constraints such as lack of impartial electoral bodies as well as free and fair elections; strict controls on rights to demonstrate and assemble; lack of truly independent judiciary; lack of good governance; non-adherence to rule of law; restriction on freedom of access of information; etc.[1150] Yet, the current political system has to be explained in a broader context of European external influence which started in the 15th century through the slave trade[1151] rather than internal dynamics whose impacts were/have not been so significant.

The abolition of slave trade in the 19th century did not leave a vacuum. It immediately saw the colonization of Africa by European powers notably the British, German, France, Portuguese, Italian and Belgian. The colonization process was preceded by the Berlin Conference of 1884-85 which partitioned Africa among these European powers. The establishment of the colonial state and its instruments that immediately came after the Berlin Conference had far reaching impacts on indigenous forms of governance. Chiefly among them was the destruction of indigenous

---

[1145] Harding, C., 'Leaving the Farm: Africa's Rapid Urbanisation', How We Made It in Africa, 12 October 2011, http://www.howwemadeitinafrica.com/leaving-the-farm-africas-rapid-urbanisation/12836/ last visited 13/02/2012.
[1146] African Business, 'Urbanisation for Better or for Worse' December 2011, Issue No.381, pp.17-24, at p.18.
[1147] Ibid.
[1148] Ibid.
[1149] Ibid, p.19.
[1150] For detailed discussion of the efficacy or otherwise of the current political system in Africa see generally Makulilo, A.B., Tanzania: A De Facto One Party State?, VDM Verlag Dr. Müller Aktiengesellschaft & Co. KG, Germany, 2008; Gentili, A.M., 'Party, Party Systems and Democratisation in Sub-Saharan Africa', Paper Presentation at the Sixth Global Forum on Reinventing Government, Seoul, Republic of Korea, 24-27 May 2005, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan020460.pdf last visited 4/02/2012.
[1151] Historians generally agree that Africa came into first contacts with Europe in the 15th century through Atlantic slave trade also known as 'Triangular Slave Trade' because of its behavioural pattern starting from Africa where slaves were sourced, proceeding to America where such slaves had to offer intensive labour force in mines and plantations owned by Europeans, then to Europe where farm and mineral products from America were finally shipped for industrial processing; and from Europe back to Africa where manufactured goods were dumped into Africa as market; see e.g. Rodney, note 96, supra; Tanzania Institute of Education., Africa from Stone Age to the Nineteenth Century, NPC-KIUTA, Dar es Salaam, 2002, p.39.

tribal leadership. Whenever the latter was tolerated to remain intact strategies to integrate it to the colonial system were made. There were several reasons. The colonial rule had its target goals namely production of raw materials for industries located in Europe, mobilization of labour force for the plantations and mines and creation of market to consume manufactured goods from Europe hence the common historical expression by African historians: 'we produce what we don't consume and we consume what we don't produce'.[1152] Concomitantly allowing the indigenous tribal rule to exist side-by-side with the colonial rule without any subjugation into the latter would have defeated the very objectives of colonialism. It was not therefore by accident that Lord Lugard, for example, introduced on behalf of the British colonial administration in Africa the so called 'indirect rule' i.e. colonial rule through the disguise of tribal rulers while slightly the French used the local chiefs and rulers as their agents.[1153]

On independence (1960s-1970s), the colonial powers introduced in Africa constitutions based on the Western style of politics and governance. These constitutions are popularly known as the 'Westminster' or 'Gaullist' constitution model after that of the United Kingdom, France or Portugal.[1154] The independence constitutions which are widely considered as 'imposed' upon the newly independent African states were tailored around the liberal constitutional principles alien to Africa. Such constitutional principles included the doctrines of separation of powers, rule of law, parliamentary supremacy, ministerial responsibility and judicial independence. Moreover multi-party political system was incorporated in the independence constitutions. Also central to these constitutions was the incorporation of the Bill of Rights which guaranteed individuals' basic rights and freedom.

However, the independence constitutions were short-lived. They were soon dismantled and replaced by totalitarian governments of military or single party regimes under the guise of socialist ideology (neither were these systems of governance indigenous to Africa).[1155] The

---

[1152] The expression was originally a summation of the nature of the colonial economy by Dr.Eric Williams the author of classic work of Capitalism and Slavery, see Girvan, N., 'The Post Colonial Economy and Society: Facing the Challenge', Paper prepared for presentation at the Regional Forum of Projects Promotion Ltd., St Vincent and the Grenadines, February 11, 2008, pp.1-16, at p.1.

[1153] For details about how the British 'Indirect Rule' operated see e.g. Crowder, M., 'Indirect Rule-French and British Style', Africa: Journal of the International African Institute, 1964, Vol.34, No.3, pp. 197-205.

[1154] See e.g., Andrew, H., 'The "Westminster Model" Constitution Overseas: Transplantation, Adaptation and Development in Commonwealth States', Oxford University Commonwealth Law Journal, 2004, Vol.4, No.2, pp.143-166; Sinjela, M., 'Constitutionalism in Africa: Emerging Trends', The Review, Special Issue, 1998, Vol.23, No.60, pp.23-29, at p. 23.

[1155] See e.g., Prempeh, H.K., 'Africa's "Constitutionalism Revival": False start or new dawn?,' International Journal of Constitutional Law, 2007, Vol.5, pp.469-506, at p.474; Wing, A.K., 'Communitarianism vs. Individualism: Constitutionalism in Namibia and South Africa', Wisconsin International Law Journal, 1992-1993, Vol.11, No.2, pp.295-380, at p.308.

collapse of independence constitutions was partly attributed to the fact that many of the assumptions underpinning them were not rooted in the African context, grounded in experience and institutionalized patterns of behaviour, nor indeed in an adequate framework of laws.[1156]

Another argument leveled against the continued existence of independence constitutions is that they were not suitable vehicle for creating unified states from different and fragmented nations often mixed in the pre-independence era.[1157] It has also been argued that a competitive system modelled after that of the Western democracies encouraged political competition and rivalry while at the same time detracted from economic development programmes set out by the independent African countries.[1158] The African nationalist elites generally discarded the independence constitutions as neocolonial devices designed to ensure 'the preservation of imperial interests in the newly emergent state.[1159] Interestingly, the post-independence Africa's military and single party regimes did not either last longer. The oil crisis of 1970s compounded by excessive draughts, civil and inter-state wars and above all the end of the Cold War resulting into the collapse of U.S.S.R in 1990s as the world superpower (once living side-by-side with the U.S.A)[1160] saw dramatic turn for developing countries including Africa. Because of economic failures attributed by those enumerated factors, African states found themselves on the mercy of the International Monetary Fund (IMF), World Bank (WB) and European donor communities in their efforts to reform the devastated economies. By 1980s the latter imposed on Africa 'structural adjustment programs' commonly known as SAPs. As part of conditions to access reliefs under SAPs African states were required to liberalize their political systems by allowing multi-party political system, democratic elections, exercise of individual rights, good governance, rule of law, accountability, etc. In short, SAPs practically required African states to return to most of the features of their independence constitutions. To achieve this African states quickly adopted either completely new constitutions or just amended the existing ones by incorporating the liberal constitutional principles. It is imperative to note that SAPs widened the space under which internal dynamics (poor living standards, legitimacy crisis, etc) would operate to mount internal pressure to the African regimes to adopt changes.

1156 Paul, J.C.N., 'Developing Constitutional Orders in Sub-Saharan Africa: An Unofficial Report', Third World Legal Studies, 1988, Vol.7, No.1, pp.1-34, at p.14.
1157 Sinjela, note 1154, supra.
1158 Ibid.
1159 The Editors of the Spark, Some Essential Features of Nkurumaism, International Publishers, New York, 1965. P.39 cited in Prempeh, p.473, note 1155, supra.
1160 The collapse of Soviet power led to the withdraw of military support to a variety of Soviet client states such as Angola. Moreover the end of Cold War reduced the geographical significance of Africa in Western eyes, because there was no longer any communist enemy to confront. Thus, western economic support for repressive anti-communist regimes lessened as well, see Wing, p.309, note 1155, supra.

As pointed out, Africa's adoption of liberal constitutions on independence and in 1980s had been pre-conditioned by foreign pressures. As a result and in practical terms such constitutions have been derailed by many African leaders. This, to some extent, explains why the executive in Africa is still very strong and not fully accountable to the people. It also explains the current election problems; lack of respect to the rule of law; interference with the judiciary; weak legislatures; weak opposition parties; problems of transparency and respect for human rights generally and basic rights and freedom of individuals. Yet, the liberal constitutions have had progressive gains in improving the political systems and life in Africa. For example, courts have so far produced a corpus of important rulings protecting civil and political liberties and limiting governmental powers.[1161] At least there are now regular elections after every four to five years in many African countries. These elections are reinforced by the rise of new era of presidential term limits.[1162] There are also ascendance of fearless and strong private media and civil societies.[1163] In some countries such as South Africa and Mauritius governments are largely made accountable to the electorates through legislatures. Moreover, some countries are moving towards the fourth generation of constitution making (after the independence constitutions; military/single party constitutions 1960s-1980s and liberal constitutions 1980s-1990s) with the view of increasingly curbing the executive powers and making the legislatures and judiciary discharge efficiently their traditional roles. This is the case with Kenya which has recently adopted a new constitution in 2010. Other countries such as Tanzania are currently undertaking constitutional review for purposes of overhauling the existing constitution enacted in 1977 but which has been amended from time to time.

Economically, Africa has evolved through pre-colonial, colonial, post-independent/neo colonial and now global economies. In pre-colonial times Africa's economy was largely subsistence. Small scale agriculture and livestock keeping were the permanent feature. Family was the main unit of labour force. Pastoralism was practiced in arid and semi-arid areas. The Maasai of the East African Valley and grassland plateau, the Fulani of Western Sudan, the Khoi Khoi of the Cape Region in South Africa, the Herero of Namibia, the Tswana of Botswana, the Galla and the Somali of the semi-desert regions of the Horn of Africa provide typical examples of pastoralist societies in Africa.[1164] Mining, industry and trade were present but limited. Technology was low and the iron technology which was invented in the first millennium A.D was used to make

[1161] Prempeh, p.502, note 1155, supra.
[1162] Ibid, p.487.
[1163] Ibid, pp.488-489.
[1164] Tanzania Institute of Education, pp.16-17, note 1151, supra.

working tools in some societies only.[1165] Starting from the 15th century, the African pre-colonial economies became incorporated into the world capitalist economy through the mercantile capitalism which saw the beginning of the Atlantic Slave Trade, and subsequently colonialism, neo-colonialism and now globalization.[1166]

Despite the above incorporation which might have positively transformed Africa, that has not been the case. The external links affected Africa adversely. Africa's economy is still characterized as pre-industrial or simply agrarian with little export trade. The national per capita income is relatively very low.[1167] Agriculture forms the largest sector of its economy but it faces many challenges due to lack of technology, viable industries, draught conditions, capital and researches. Together Africa accounts for less than 2% of the global trade.[1168] The industrial and mineral sectors as well as tourism have yet been fully realized although the continent is rich in these natural resources. In the period following independence the state was in total control of economy. The private sector was very weak. However with SAPs which came about in 1980s strict terms were imposed on African states by the IMF, World Bank and Africa's lenders and creditors of the last resort, as a condition for providing interim relief, to liberalize and deregulate their economies and structure their public administrations; privatize the loss-making state enterprises, remove price controls and subsidies for the social services, and trim blotted public payrolls.[1169] The economic liberalization has resulted into significant growth of the private sector in present day Africa. It has also changed the pattern of ownership. The latter in turn has led to the individual ownership of property.

Technologically, Africa has come far away. Walter Rodney asserts that in the 15th century when Africa first came in contact with Europe, the latter's technological development was not superior to that of Africa and the rest of the world generally.[1170] Yet, he notes that there were certain specific features that were highly advantageous to Europe such as shipping industry and (to a lesser extent) guns.[1171] According to this historian, Africa had strength in the cloth industry and

---

[1165] Ibid, p.18.
[1166] See e.g., Henriot, P.J., 'Globalisation: Implications for Africa', http://sedosmission.org/old/eng/global.html last visited 18/02/2012; Olutayo, A.O and Omobawale, A.O., 'Capitalism, Globalisation and the Underdevelopment Process in Africa: History in Perpetuity', African Development, 2007, Vol.32, No.2, pp.97-112, at pp.100-106.
[1167] See e.g., World Bank., 'Gross National Income Per Capita 2010, Atlas Method and PPP', 2011, http://siteresources.worldbank.org/DATASTATISTICS/Resources/GNIPC.pdf last visited 5/02/2012.
[1168] Arieff, A *et al.*, 'The Global Economic Crisis: Impact on Sub-Saharan Africa and Global Policy Responses', CRS Report for Congress, 2010, p.8, http: //www.fas.org/sgp/crs/row/R40778.pdf. last visited 5/02/2012.
[1169]Prempeh, p.483, note 1149, supra.
[1170] Rodney, p.103, note 96, supra.
[1171] Ibid.

irrigation technology (e.g. North Africa particularly Egypt).[1172] However, through the Atlantic slave trade that saw the decline of Africa's skilled labour force and colonialism Africa lost its technological grip. Under colonialism, Africa remained the exporter of raw materials as well as importer of manufactured goods from Europe. This explains why, for example, the African cotton cloth industry declined as a result of competition from importing manufactured cotton cloth which were of cheap and of high quality.[1173] Accordingly, this remarkable reversal is tied to technological advance in Europe and to stagnation of technology in Africa owing to the very trade with Europe.[1174] Yet while Europe has its share in the Africa's 'technological arrest,' after independence, African nationalist elites fueled the regression. This is because, immediately after independence most African countries purporting to completely detach from European influence and in view of stimulating industrialization in the newly independent states banned imports from Europe.[1175] While it was thought this could have boosted local technological development and industries, the same failed to produce such effect. Instead such protectionist policies greatly constrained Africa's ability to participate in international trade.[1176] As a result, technologically the continent has remained backward compared to the rest of the world, particularly Europe and America. However two caveats need to be made. First, when a society for whatever reason finds itself technologically trailing behind others, it catches up not so much by independent inventions but by borrowing.[1177] Japan is widely cited as an example of a country which effectively borrowed technology from Europe and became capitalist.[1178] Yet this could not happen in Africa despite centuries of contact with Europe because of the nature of the relationship between the two continents which operated in disfavor of the former.[1179] The second caveat partly linked to the first is that technology transfer should be distinguished from transplantation. Whereas in the former case, the demand for European technology would have come from inside Africa with the willingness of both sides[1180] the latter involves the imposition of such technology from Europe to Africa. As a result, customization of such technology to suit the local needs has been difficult. Undoubtedly, this second caveat has contributed to Africa's resistance to embracing imported technology.

[1172] Ibid, pp.41 and 103.
[1173] Ibid, pp.103-104.
[1174] Ibid, p.104.
[1175] Martin, W., 'Trade Policies, Developing Countries and Globalisation', Development Research Group, World Bank, 9 October 2001, pp.1-35, at p.8,
http://siteresources.worldbank.org/INTPRRS/Resources/2866_trade_martin.pdf last visited 15/02/2012.
[1176] Ibid.
[1177] Rodney, p.106, note 96, supra.
[1178] Ibid.
[1179] Ibid.
[1180] Ibid.

However, Africa's technological breakthrough in the formal sense started with the lifting of protectionist policies in 1980s-1990s following SAPs. Through trade liberalization African countries began to import technology from developed countries particularly Europe. Today Africa has realized the importance of technology as the basis of creating an information economy.[1181] Recent statistical records by the International Telecommunication Union (ITU)[1182] indicate that Africa is the region with the highest mobile phone growth rate. By the end of 2008, it had 246 million mobile subscriptions compared to the five million mobile cellular subscriptions in 2000; and mobile penetration has risen from just five per cent in 2003 to well over 30 per cent by 2009.[1183] The number of Internet users has also grown faster than in other regions.[1184] Yet, despite rapid growth, Africa's ICT penetration levels in 2009 was still far behind the rest of the world and very few African countries reach ICT levels comparable to global averages.[1185] Less than five per cent of Africans use the Internet, and fixed and mobile broadband penetration levels are negligible.[1186] It is noteworthy that the pattern of ICT infrastructure in Africa has left a 'digital divide' between urban and rural areas with high ICT concentration in the former.[1187] Yet efforts to bridge the gap are being made although with some slow progress.[1188]

Socially, Africans' ways of life have been greatly affected by political, economic and technological liberalism. Prior to external contacts with Europe in the 15th century and generally in pre-colonial era, Africans were predominantly living in kinship and other closely associated groups.[1189] In such socio-political organizations, individuals lived in interdependence. This relationship between an individual and another in the African community has been expressed in summary in a famous Zulu/Xhosa proverb: *umuntu ngumuntu ngabantu abanye* (i.e. a person is a person through

[1181] See e.g., Molla, A., 'Downloading or Uploading? The Information Economy and Africa's Current Status', Information Technology for Development, 2000, Vol.9, No.3 & 4, pp.205-221.
[1182] International Telecommunication Union., 'The Information Society Statistical Profiles 2009:Africa', p.ii, http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-RPM.AF-2009-PDF-E.pdf last visited 5/02/2012.
[1183] Ibid.
[1184] Ibid.
[1185] Ibid.
[1186] Ibid.
[1187] See e.g. Alemna, A.A and Sam, J., 'Critical Issues in Information and Communication Technologies for Rural Development in Ghana', Information Development 2006, Vol.22, No.4, pp.236-241; Fuchs, C and Horak, E., 'Africa and the Digital Divide', Telematics and Informatics, 2008, Vol.25, No.2, pp.99-116.
[1188] See e.g., Kasusse, M., 'Bridging the Digital Divide in Sub-Saharan Africa: The Rural Challenge in Uganda', The International Information & Library Review, 2205, Vol.37, No.3, pp.147-158, at p.157; Gebremichael, M.D and Jackson, J.W., 'Bridging the gap in Sub-Saharan Africa: A holistic look at information poverty and the region's digital divide', Government Information Quarterly 2006, Vol. 23, No.2, pp.267-280, at p.272.
[1189] See e.g., Ezedike, E.U., 'Individualism and Community Consciousness in Contemporary Africa: A Complementary Reflection', Sophia: An African Journal of Philosophy, 2005, Vol.8, No.1, pp.59-64, at p.61.

other persons). The shorthand of this proverb is commonly cited as *Ubuntu*.[1190] The latter's core values include aspects like communalism, interdependence, humanness, sharing, compassion, respect and caring.[1191] Mbiti, a Kenyan famous philosopher, has underscored the African relationship in the following expression: 'I am because we are, and since we are therefore I am'.[1192] Yet, although *Ubuntu* philosophy has its roots in South Africa it has been popularized as representing African worldview.[1193] Some scholarships have only regarded it as the most recent manifestation of the notion of an African humanism, similar to earlier notions such as Pan-Africanism, *Ujamaa* (i.e. the special type of socialism in Tanzania) or *negritude*[1194] especially after the collapse of the latter. They have therefore dismissed *Ubuntu* as a post-colonial 'Utopia' invention and/or a 'prophetic' illusion crafted by the African political elites in the age of globalization.[1195]

From the preceding discussions, the dominant discourse by African and non-African scholars tend to claim that Africans have only been collectivists.[1196] Yet, individualism and individualistic life style could/can still be identified in the pre-colonial African societies and the subsequent periods. This point is well articulated by Professor Olufemi Taiwo who posits:-

> 'Africans and non-Africans alike believe that African societies are essentially communalistic and are fundamentally reluctant to pollute these waters with an introduction of the bad philosophy of individualism. This is a misplaced identification. It ignores the fact that what needs to be accounted for when we investigate social forms are what type of individualism can be found in various societies, what indigenous nodes of individualist transformations are there to be isolated, and how those nodes were affected by colonialism. What is at issue is not whether there were forms of individualism in any but the most primitive societies but what kind of individualism there is and what role it plays in social ordering. In addition a blanket condemnation of individualism reinforces a reluctance to identify its presence in African societies, past and present. I abjure such a blanket condemnation. While this is not the place to

[1190] See the meaning of *Ubuntu* in note 65, supra.
[1191] Olinger *et al*, pp.34-35, note 64, supra.
[1192] Mbiti, J., African Religions and Philosophy, Heinemann, London, 1969, p.144.
[1193] See e.g., McDonald, D.A., 'Ubuntu Bashing: The Marketisation of "African Values" in South Africa', Review of African Political Economy, 2010, Vol. 37, No.124, pp.139-152, at pp. 141-142.
[1194] McAllister, P., 'Ubuntu-Beyond Belief in South Africa', Sites: New Series, 2009, Vol.6, No.1, pp.1-10, at p.2.
[1195] Nabudere, D.W., 'Ubuntu Philosophy: Memory and Reconciliation', 2008, pp.1-20, at p.1, http://www.grandslacs.net/doc/3621.pdf last visited 10/02/2012.
[1196] See e.g., the collectivist-individualism strand in 1.2.1 of this thesis.

> consider the many sides of individualism, I must insist that its introduction into African societies by the apostles of modernity and its evolution in indigenous societies following upon their own internal dynamics deserve serious scholarly attention that does not preclude condemnation of its deleterious consequences if there have been such.'[1197]

The above paragraph clearly suggests that some forms of individualism existed in pre-colonial African societies independent from external influences. Taiwo's views are collaborated by Ezedike who argues:-

> 'At the same time, let it be said here, that African communitarianism is not unqualified collectivism. It would be unbalanced and naive assessment to portray the African traditional community as a totalitarian community in which an individual is a mere pawn within the rigid and ruthless set-up. What we are saying is that the idea of community consciousness should not be interpreted to mean that an individual is completely submerged in the collectivism and thus has no rights, personal initiatives nor any sense of self-reliance. This would certainly amount to exaggeration and distortion of facts. An individual can hardly be regarded as a slave to community.'[1198]

Taiwo and Ezedike's views are reiterated by Kigongo. The latter holds that in African traditional society social cohesion was dominant over individuality; unlike individualism, it seems to have been distinctly discernible.[1199] It is imperative to mention that the co-existence of collectivism and individualism in pre-colonial societies is similarly pondered by two renowned African philosophers Kwame Gyekye and Leopold Senghor. Gyekye observes, 'it would be more correct to describe that order (i.e. African social order) as amphibious, for it manifests features of both communality and individuality….African social thought seeks to avoid the excesses of the two exaggerated systems, while allowing for a meaningful, albeit uneasy, interaction between the individual and the society'.[1200] In tandem with Gyekye, Senghor regards traditional African

---

[1197] Taiwo, O., Colonialism Pre-empted Modernity in Africa, Indiana University Press, U.S.A, 2010, p.85.
[1198] Ezedike, note 1189, supra.
[1199] Kigongo, J.K., 'The Concept of Individuality and Social Cohesion: A Perversion of Two African Cultural Realities' in Dalfovo, A.T *et al* (eds)., The Foundations of Social Life: Uganda Philosophical Studies, I, The Council for Research in Values and Philosophy, Washington, 1992, pp.59-68, at p.59.
[1200] Gyekye, K., The Unexamined Life: Philosophy and the African Experience, Ghana University Press, Accra, 1988, pp.31-32 cited in Lassiter, J.E., 'African Culture and Personality: Bad Social Science, Effective Social Activism, Or a Call to Reinvent Ethnology?', African Studies Quarterly, 2000, Vol.3, No.3, pp.1-21, at pp. 5-6.

society to be 'based both on the community and on the person and in which, because it was founded on dialogue and reciprocity, the group had priority over the individual without crashing him, but allowing him to blossom as a person.'[1201]

During the colonial period, the African social relationship experienced stronger external shock of waves than those in the slave trade. Western education and Christianity played significant role in impacting on the African social cohesion. With colonial education and religion, western values based on individualism slowly permeated into African cultures making *Things Fall Apart*[1202] or creating *The River Between*[1203] as some African literature writers have portrayed the effect of colonialism in their fiction. Apart from education and religion, the colonial government and the colonial economy exerted enormous pressures on the African cultural life. Under colonialism almost every individual was forced into the colonial monetary system and economy by provision of labour force which sometimes displaced families (in case of labour migration), payment of taxes, etc. This point is well underscored by Okigbo with respect to the impact of colonialism in West Africa where he observed that the family and kinship structures showed signs of breaking down as a result of the impact of the growing individualism.[1204]

In postcolonial period, the external forces continued to erode the African social forms in the direction of individualism. First, the leaders and African scholars of the African independence and post-independence era analyzed the African value system with socio-economic and political implications that are drawn from a different value system, Marxism.[1205] The former used African value system as justification for their choice of Marxist socialism.[1206] The latter was the dominant ideology in Africa shortly after independence yet it was alien in the continent although it was similar to African value system. Second, and perhaps the most important, following the collapse of world's socialist system, Africans are now engaged in the process of completely abandoning their value system and attempting to embrace liberalism.[1207] Under liberalism Africans are living

---

[1201] Senghor, L., 'Negritude' in Optima, 16:8, 1966 cited in Lassiter, J.E., 'African Culture and Personality: Bad Social Science, Effective Social Activism, Or a Call to Reinvent Ethnology?', African Studies Quarterly, 2000, Vol.3, No.3, pp.1-21, at pp. 5-6.
[1202] Achebe, pp.123-125, note 144, supra.
[1203] Wa Thiong'o, N., The River Between, East African Educational Publishers Ltd, Nairobi/Kampala/Dar es Salaam, 2007, under licence from Heinemann Educational Books Ltd, UK.
[1204] Okigbo, P., 'Social Consequences of Economic Development in West Africa', The Annals of the American Academy of Political and Social Science, 1956, Vol.305, pp.125-133, at pp.132-133.
[1205] Ntibagirirwa, S., 'A Wrong Way: From Being to Having in the African Value System' in Giddy, P(ed)., Protest and Engagement: Philosophy after Apartheid at an Historically Black South African University, South African Philosophical Studies, II, The Council for Research in Values and Philosophy, Washington, 2001, pp.65-81, at p.65.
[1206] Ibid, p.70.
[1207] Ibid, note 1205, supra.

in societies in which everything is permitted under the name of individual freedom and autonomy.[1208] The Kenyan rural sociologist Preston Chitere, offers the following observation regarding the current state of the African family in Kenya, a state or condition that exists in many other sub-Saharan African nations:-

> 'The effects of capitalism are already being felt in our families. Individualism in society is increasing. Even families in rural areas like to operate in isolation, and those who offer any help are keen to help their immediate families only. The (conjugal) family is becoming more independent. The loss of community networks and the development of individualism have resulted in (increased occurrences of) suicide, loneliness, drug abuse and mental illness. The communal system is breaking down. The extended family had certain functions to perform, for instance, to reconcile couples at loggerheads with each other, but this is no longer the case. It is no one (else's) business to know what's happening in one's marriage today.'[1209]

In support of the above observations but in the Nigeria context, Omobowale observes that since the incorporation of the Nigerian economy into the world capitalist system, the indigenous social structure has been fundamentally restructured with the youth being immensely immersed in Western cultures.[1210] Recent empirical studies carried out in different parts of Africa have confirmed the above observations. Suffice here to mention four of them in order to make this point clearer.

The first of the above studies: *Individualism versus Community in Africa? The Case of Botswana*[1211] was carried out in Botswana to answer the following question: How is it possible that two deeply-rooted values in some African societies-the people's sense of individualism and their sense of community-have persisted through time when they seem to work against each other?[1212] This study was carried out in the context of collective and private government-sponsored farming

---

[1208] Ibid, p.74.
[1209] See, Kimani, P., 'When the family becomes a burden', Daily Nations, Weekender Magazine, 23 January 1998, p.1 cited in Lassiter, p.9, note 1178, supra; see also, Edwards, C.P and Whiting, B.B (eds)., NGECHA: A Kenyan Village in a Time of Rapid Social Change, University of Nebraska Press, Lincoln/London, 2004; Sindima, H., 'Liberalism and African Culture', Journal of Black Studies, 1990, Vol.21, No.2, pp.190-209.
[1210] Omobowale, A.O., 'The Youth and the Family in Transition in Nigeria', Review of Sociology, 2006, Vol.16, No.2, pp.85-95, at pp.85 and 90.
[1211] Roe, E.M., 'Individualism versus Community in Africa? The Case of Botswana', The Journal of African Modern Studies, 1988, Vol.26, No.2, pp.347-350.
[1212] Ibid, p.347.

projects in rural areas. The study found that it is not that the African value of individualism undermines the chances of success for government-sponsored group efforts, or that the African value of community hampers the successful operation of government-initiated efforts to promote private enterprises.[1213] Rather what works against these endeavors in many rural areas is that they involve taking risks, when the cultural context in which they are meant to operate, both at the individual and societal levels, has been profoundly averse to taking such risks.[1214]

The second study was carried out in Kenya: *Individualism versus Collectivism: A Comparison of Kenyan and American Self-Concepts*.[1215] This study involved two levels of comparison of self-concepts in relation to culture. The first level was a comparison between Kenya and America in which case it was fond that conceptions of the self among the pastoral nomads in Kenya are more collective and less individualized than Western or American self-concepts.[1216] This first level confirmed the researchers' hypothesis as it was expected. The second level of comparison involved the various groups and communities within Kenya. As compared to Kenyans living in rural areas especially the Maasai, the study found that factors of urbanization, development, modernization and Western education influenced the self-concepts of Kenyans living in Nairobi (the capital city of Kenya) and resulted in a decreased level of collectivism.[1217]

The third empirical study was carried out in Swaziland under the title: *The Indigenous Rights of Personality with Particular Reference to the Swazi in the Kingdom of Swaziland*.[1218] This research study found among other things that the rural areas of Swaziland have never remained static.[1219] Instead, considerable pressure has been exerted on traditional Swazi structures by large agri-business, medical and educational missionaries leading to modernization and transformation of traditional rural populations.[1220] More specifically, industrialization and urbanization with the accompanying labour migration have eroded the ties of kinship with the result that women alone have been obliged to rear families, with modern Swazi households lacking the establishing

---

[1213] Ibid, p.349.
[1214] Ibid.
[1215] Thomas, V.M and Schoeneman, T.J., 'Individualism versus Collectivism: A Comparison of Kenyan and American Self-Concepts', Basic and Applied Social Psychology, 1997, Vol.19, No.2, pp.261-273.
[1216] Ibid, p.269.
[1217] Ibid.
[1218] Ferraro, G., 'Rural and Urban Population in Swaziland: Some Sociological Considerations', National Symposium on Population and Development, 26-29 May 1980, Mbabane, Swaziland, at p. 3 cited in Anspach, P., 'The Indigenous Rights of Personality with Particular Reference to the Swazi in the Kingdom of Swaziland', PhD thesis, University of South Africa, 2004, pp.52-53.
[1219] Ibid.
[1220] Ibid.

influence of a patriarchal head.[1221] Accordingly, the foundation and social cohesion upon which the family and kinship ties were based upon had collapsed.

The fourth study illustrating the diminishing value of collectivism in Africa was carried out in Malawi.[1222] This study is interesting as it specifically investigated the existence of *Ubuntu* in Malawi's political system. It found that the dictatorial regime of the then President Kamuzu Banda associated with massive corruption; violation of individuals' rights, embezzlement of public resources, torture, political killings, mysterious deaths, etc denied the regime of any *Ubuntu* standards.[1223] These findings are relevant to other African countries in which the governments are corrupt, lack transparency, are not accountable to the people, they are self-enriching and do not respect individuals' rights.

Under globalization, African culture of collectivism has to a large extent given way to Western individualism. Maduagwu argues that the present-day extreme individualism of the West, the outcome of centuries of laissez-faire capitalism, is being transmitted across the world as the final stage of world civilization to which all cultures must strive to attain.[1224] It is elucidated that the communication dimension of globalization has the potential of eroding national cultures and values and replacing them with the cultural values of more technologically and economically advanced countries, particularly the United States and members of the European Union.[1225] People living in the urban centers, towns and large cities of Africa are currently experiencing the rapid growing of Western individualism.[1226] Rural areas of Africa are also slowly being drawn in individualism.[1227]

4.3 African Culture of Privacy

Perhaps it is intriguing to commence discussion in this section with the remarks of the Nigerian Professor Nwauche:-

---

[1221] Ibid.
[1222] Tambulasi, R and Kayuni, H., 'Can African Feet Divorce Western Shoes? The Case of "Ubuntu" and Democratic Good Governance in Malawi', Nordic Journal of African Studies, 2005, Vol.14, No.2, pp.147-161.
[1223] Ibid, p.149.
[1224] Maduagwu, M.O., 'Globalization and Its Challenges to National Culture and Values: A Perspective from Sub-Saharan Africa', in Köchler, H(ed)., Globality versus Democracy? The Changing Nature of International Relations in the Era of Globalization, Jamahir Society for Culture and Philosophy, Vienna, 2000, pp.213-224, at p. 216.
[1225] Ibid, pp.213-214.
[1226] Thomas, note 1217, supra; see also, Newell, S., 'Corresponding with the City: Self-help Literature in Urban West Africa', Journal of Postcolonial Writing, 2008, Vol.44, No.1, pp.15-27.
[1227] See e.g., Kimani, note 1209, supra; Ferraro, note 1218, supra.

> 'Is privacy important in Nigeria? The answer to the question is Yes. Because there are human beings in Nigeria. And there is a constitutional protection of this right. Yet as we have noted above this is one right that has not received adequate protection or elaboration both in the definition, philosophical basis or the key issues in the concept of privacy.'[1228]

As a departure, Nwauche's contention considers the existence of human beings in Nigeria (and in every African country) as a pre-condition for existence of the value to privacy. His views are based upon dignitary concept of personality and self worth of a person. Nwauche argues that dignitary concept seeks to protect the personality of an individual because he is a human being.[1229] He holds that this is the broader basis of human rights.[1230] Accordingly, dignitary interests, on the one hand recognize the individual autonomy of person and the need to respect such autonomy flowing from the dignity of a person.[1231] On the other hand dignitary interests are related to the self worth of a person as such the law seeks to protect an individual's subjective feelings.[1232] There is yet another reason that Nwauche advances regarding the existence of the value of privacy in Nigeria and Africa generally: the availability of constitutional protection of the right to privacy. Generally considered, Nwauche's views partly settle the question whether privacy exists or is an important value in Africa.

In contrast to Nwauche, Olinger *et al*'s survey of *Ubuntu* (i.e. the African culture based on collectivism) reveals that privacy does not exist in African culture because in such culture individuals' interests are inferior to the group.[1233] As a result an individual cannot advance claims for individual's right of privacy. This survey finds support of Burchell.[1234] However in Swaziland, the Swazi indigenous culture seems to recognize privacy, although not in Western individualist sense, in the right of honour or dignity.[1235] Yet this privacy recognition is flimsy. As a result there is no African word corresponding squarely to the English word privacy.

The above background leaves it clear that African culture of privacy is largely a byproduct of external influence from the West. The clearest initial point through which privacy started to take

[1228] Nwauche, p.66, note 179, supra.
[1229] Ibid, p.65.
[1230] Ibid.
[1231] Ibid.
[1232] Ibid.
[1233] Olinger *et al*, note 64, supra.
[1234] Burchell, note 77, supra.
[1235] Anspach, pp.217-218, note 1218, supra.

shape in Africa was in 1960s-1970s.[1236] This was the period when most African states became independent from their European colonizers. Through independence constitutions (i.e. the first generation of liberal constitutions) 'privacy' found its existence in Africa in the Bill of Rights incorporated in most of such constitutions. Yet, the Bill of Rights generally and the 'privacy' right specifically had little impact on the lives of the people during this period. A complex array of factors offers explanation to this state of affair. The African ruling elites deliberately ignored Bill of Rights by erroneously thinking that its enforcement would be incompatible with implementation of development programmes which were at stake; lack of culture of respect of individual rights which was most invariably not in harmony with the African culture of collectivism and non-involvement of African people in the independence constitutional making process leaving out the impression that such constitutions and whatever values they cherished were out of touch of African soils henceforth externally oriented and imposed on Africans. The diminishing importance of Bill of Rights at this time became apparent following the adoption of military and single party dictatorial regimes shortly after independence. In the atmosphere where the Bill of Rights was absent or had very little role to play, the right to privacy became virtually absent and accordingly privacy could not be claimed even if one would have wished to do so.

Privacy as a right reappered in 1980s-2000s. This period saw the return of the liberal democratic constitutions incorporating Bill of Rights with 'privacy' as one of its components. Otherwise this period is regarded as the second generation of liberal constitutions in Africa. With such constitutions the concepts of liberal Western values as well as privacy significantly permeated in African consciousness and culture. More importantly, 'privacy' consciousness has been catalyzed by specific factors operating in wider environment of socio-economic, political and technological set up of Africa from 1980s to 2000s. These set of factors are considered below as determinants of privacy concerns.

4.3.1 Determinants of Privacy Concerns in Africa

Privacy concerns which means desire to keep personal information to one-self are essential in determining the adoption of privacy policies and legislation. Such concerns are influenced by various factors in Africa. These can be broadly classified as positive or negative determinants. The former relate to factors which operate to cause individuals to be concerned with their privacy and possibly make claim for its protection. It is less important if those factors themselves

[1236] South Africa presents an exceptional trend whereby the recognition of 'privacy' as an independent right came much earlier in 1950s than in the rest of other African countries (see Chapter 6).

are positive or negative in their nature but produce one similar result: causing people to be concerned and value their privacy. The other class of determinants is the negative determinants in the strict sense. The latter constitute factors operating as impediments to the growth of privacy attitude. Both sets are considered below. However before this examination is undertaken it is imperative to consider their nature.

Characteristically, privacy determinants in Africa are either spontaneous or non spontaneous in operation and in producing their effects. Also, some of them are either localized in a particular country or sub-region while others have region-wise influence. Moreover, one or more determinants may operate simultaneously or otherwise in shaping and reshaping privacy attitudes. Important also to point out is the magnitude of these determinants. Quite often the determinants of privacy concerns produce effects at varying degrees: high and low degrees. However this does not suggest undermining the significance of the latter.

One caveat must be read in the above classification of determinants of privacy concerns. The classification presented here is undeniably not universal. Neither is it exhaustive. Yet, it serves to delineate the current major catalysts of privacy concerns in Africa. These may be the bases for policy and legislative developments. Also considering these determinants as not exhaustive leaves open for future determinants to arise and shape and reshape privacy attitudes in Africa.

4.3.1.1 Positive Determinants

- **Development of Databanks**

Much of the present day ICTs in Africa is a result of importation of technology mainly from Europe, the United States and currently from China. Illustrations of such technologies include computer hardware and software, mobile handsets including smart phones, TV sets, DNA machines, DVD recorders and players, Internet facilities, body scanners, etc. While these ICTs have been essential tools for information communication making Africa part of the famous 'global village' they have at the same time posed a number of risks on individuals' personal information. One of the ways in which personal information is apparently threatened by ICTs is the African governments' tendencies of creating large databanks for various purposes. The latter have manifested mainly in the form of mandatory registration of SIM cards in which all service providers were and are still required as part of their licensing conditions to register all subscribers

using their networks. The countries which have so far implemented mandatory SIM cards registration include Tanzania, Kenya, Nigeria, Botswana, Ghana, Mozambique, South Africa, Zimbabwe, Burundi, Rwanda, Gambia, Sierra Leone, Liberia, Algeria, Cameroon, Cote d'Ivoire(Ivory Coast) and Uganda. In most cases, registration of SIM cards in such countries requires subscribers to furnish a wide range of their personal information. For natural person, information required include names, phone number, gender, date of birth, marital status, residential or business address, employment details, identity number or other document which proves identity of the subscriber, alternative mobile phone number(if any), subscriber's photograph, etc. However in case of non-natural person usual information required include registration number accompanied by certificate of registration or incorporation, business license and tax payers identification number(TIN). In either case, unspecified additional information relating to the subscribers can be asked by those persons registering subscribers on behalf of the service providers.

The development of SIM card databanks has sparked public debates over concern for privacy. Part of the reason is the fact that in many countries such as Tanzania, Kenya, Nigeria, Ghana and Botswana, to mention but few examples, the mandatory registration of SIM cards proceeded on the basis of administrative directives from the national communication authorities in the respective countries.[1237] There was no in place any legislation or regulation for guiding the entire registration process including how subscribers' privacy would be guaranteed. Such administrative directives are generally vague and their scope unclear. Moreover the latter's legal status and enforcement has quite often been challenged.[1238] Even when legislation or regulations for SIM card registration were in place before or after, most of them have left many potential loopholes for infringing subscribers' personal information.[1239] Also, a wide range of personal information has been collected without any proper verification risking these databases to contain inaccurate information.[1240] As an illustration, the National Communications Authority (NCA) in Ghana revealed that about 5.2 million consumers registered have invalid data.[1241] There is also ample

[1237] See e.g., Makulilo, p.48, note 225, supra; Murungi, M., 'Registration of Mobile Phone Users: Easier said but carefully done', Kenya Law, 26th July 2009, http://kenyalaw.blogspot.com/2009/07/registration-of-mobile-phone-users.html last visited 19/02/2012; Izuogu, note 180, supra; Anan, K., 'What is My Beef Against SIM Card Registration in Ghana?, Independent Civil Advocacy Network, 25th January 2010, http://www.i-can-ghana.com/?p=104 last visited 19/02/2012; Sutherland, E., 'The Mandatory Registration of SIM Cards', Computer and Telecommunications Law Review, 2010, Vol.16, No.3, pp.61-63, at p.61.
[1238] Ibid.
[1239] See e.g., Makulilo, pp.50-54, note 225, supra; Hemeson, C.J., 'Directive on Consumer Data for SIM card Registration in the Telecommunications Sector: An African Perspective', Social Science Research Network, 2012, pp.1-12, at p.5, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1982033 last visited 22/02/2012.
[1240] Sutherland, p.63, note 1237, supra.
[1241] Hemeson, p.6, note 1239, supra.

evidence for the misuse of personal information in the subscribers' databases in some jurisdictions (see e.g. chapter 7). Mobile spying, interception and everdrop on digital cell phones conversations and other abuses relying on individuals' personal information are commonplace despite the mandatory registration of SIM cards. This has casted doubts on the efficacy of such laws and also creating fears of 'big brothers', 'little brothers' and 'little sisters'.[1242]

The other manifestations of systems of database in Africa include those on identification systems (ID Systems). These constitute the most common ICT privacy issue currently facing Africa.[1243] Such ID systems either manifest as national identification cards (National ID cards) leading to creation of databanks of all nationals in a particular country or passports.[1244] Both systems use biometric technology. Concerns for privacy in this context have arisen from the fact that many of the ID systems such as the ones in Rwanda and Mozambique (and now Tanzania) are developed and operated by foreign companies.[1245] While there is no concrete evidence of any misuse of personal data, these concerns have tended to rest upon little control by the African governments to prevent such companies from transferring information outside their respective jurisdictions or deal with it in an incompatible manner. As a result, it is feared that companies may misuse personal information at the peril of individuals. Yet significant concerns come from security issues as well as reliability of these databases.[1246] Rwanda and Kenya serve as typical illustrations of misuse of personal information based on ID systems. During the Rwandan genocide of 1994 the national ID cards were used to identify the 'Tutsi' victims. Jim Fussel explains how important the identification cards were in facilitating the Rwandan genocide of which the International Criminal Tribunal for Rwanda based in Arusha-Tanzania was established to try the culprits. Fussel posits:-

> 'In 1994 genocide in Rwanda began, an ID card with the designation "Tutsi" spelled a death sentence at any roadblock. Along with the prior training of militias, stockpiling of weapons, direction of the massacres by hate radio, the prior existence of ethnic ID cards was one of the most important factors

[1242] See e.g., Makulilo, note 225, p.49 (footnote 11); Hemeson, p.7, note 1239, supra.
[1243] Banisar, D., 'Linking ICTs, The Right to Privacy, Freedom of Expression and Access to Information', East African Journal of Peace & Human Rights, 2010, Vol.16, No.1, pp.124-154, at p.126.
[1244] Ibid.
[1245] Ibid.
[1246] Ibid.

> facilitating the speed and magnitude of the 100 days of mass killing in Rwanda.'[1247]

Although the national ID card system in Rwanda was introduced in 1933 way back in Belgian colonial days when ICTs were uncommon, the modern ID systems tend to rely on the same pattern yet based upon sophisticated technologies. This has increased many risks of abuses of personal information. Closely similar to Rwanda is Kenya. The latter's post election violence in 2007 which saw a death toll of more than 1,000 people relied on IDs to identify certain ethnic groups the price of which some senior members of the current Kenyan government are to pay by facing trial for international crimes in The Hague.[1248]

Alongside the subscribers' databases for mobile phones and national ID cards, there are also in many African countries centralized voter registration databases (CVRD). Some of the countries with CVRD include Tanzania, Ghana, Liberia, Malawi, Zambia, Mozambique, Rwanda, Senegal, and Democratic Republic of Congo (DRC). The CVRD are in many cases computerized databases with biometric information most invariably fingerprints. Privacy concerns with regard to CVRD have been raised in three main areas. First, most African countries do not have comprehensive data privacy legislation neither do such countries have legislation nor regulations which authorize collection of voters' personal information while guaranteeing protection of privacy.[1249] Second, where voter registration involves biometrical registration, individuals' concerns for privacy have been raised high. The current registration of voters in Ghana for the 2012 election is illustrative. In connection with this, some commentators have argued that since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods, however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.[1250] Third, personal information collected for voting purposes are in most cases shared and re-used for other purposes. This is especially in countries where there are no national IDs. In Ghana, apart from voters' ID cards being used by card holders for private transactions, the same cards have been widely recognized

---

[1247] Fussel, G., '*Indangamuntu* 1994: Ten years ago in Rwanda this Identity Card cost a woman her life', Prevent Genocide International, http://www.preventgenocide.org/edu/pastgenocides/rwanda/indangamuntu.htm#intro last visited 19/02/2012; see also Santon, G.H., 'Could the Rwandan Genocide have been prevented? Journal of Genocide Research, 2004, Vol.6, No.2, pp.211-228, at p. 214.

[1248] See e.g., Banisar, p.127, note 1243; PA., 'Senior Officials to face ICC Trial over Kenya Violence', The Independent, 23rd January 2012, http://www.independent.co.uk/news/world/africa/senior-officials-to-face-icc-trial-over-kenya-violence-6293413.html last visited 19/02/2012.

[1249] Evrensel, A., 'Introduction', in Evrensel, A(ed)., Voter Registration in Africa: A Comparative Analysis, Electoral Institute for the Sustainability of Democracy in Africa(EISA), Johannesburg, 2010, pp.1-54, at p.16.

[1250] Asmah, K., 'Let's Commit To Biometric Registration', Daily Graphic, 20th January 2012, http://www.graphic.com.gh/dailygraphic/page.php?news=18417 last visited 19/02/2012.

and accepted as official identification by various institutions.[1251] This is also the case with many other African countries which have not yet adopted national ID card registration system. The privacy issue arising here is that at the time of registration and hence collection of personal data, the respective individuals are not made aware of disclosure of their personal information to third party institutions or individuals for purposes other than voting. Yet, in defending the practice, the electoral commissions which are the custodians of individuals' personal data have always argued that since voters voluntarily use voters' registration cards for other transactions, they have by virtue of that given permission for their personal data to be exchanged between those institutions and voters' roll databases.[1252]

Other databases that are fast developing in Africa include DNA databases, biometric databases and body scanners. Various jurisdictions in Africa such as Mauritius and Tanzania have adopted legislation on DNA profiling. However in many instances these pieces of legislation contain inadequate safeguards to guarantee protection of privacy raising individuals' concerns over their privacy.[1253] This is also the case with biometric databases like those used in issuing biometric passports. Normally the immigration and/or passport legislation in Africa under which those passports are issued require applicants to be taken samples of their fingerprints and sometimes their irises. However, quite often such laws fail to provide proper safeguards of biometrical materials raising concerns for privacy.[1254] Body scanners which have wider privacy implications have similarly started to be put in use in African airports and other places. For example, after the 2009 attempted Christmas Day bombing by a Nigerian terrorist Umar Farouk Abdulmutallab, the Nigerian government ordered N448 million worth of body scanners to be installed in Nigerian airports.[1255] Similarly, last year the Nigerian National Assembly advertised contracts for procurement of full-body scanners which would be fixed at the buildings in the precincts of the legislature.[1256] Also, the procurement was intended to acquire bomb detectors and electronic surveillance equipments.[1257] It is imperative to point that these technologies have far reaching

[1251] Evrensel, pp.16-17, note 1249, supra.
[1252] Ibid.
[1253] For further discussion see chapters 5 and 7 of this thesis respectively.
[1254] See e.g., Williams, R., 'Doubts over Biometric Passports', Habari Tanzania, 27th October 2005, http://www.habaritanzania.com/new/articles/1945/1/-Doubts-over-biometric-passports last visited 20/02/2012.
[1255] Nwezeh, K and Eze, C., 'Nigeria: Abdulmutallab-Ministers, Foreigners to Undergo Full-Body Scan', This Day, 27th January, 2010, http://allafrica.com/stories/201001270590.html last visited 20/02/2012; see also Banisar, p.128, note 1243, supra.
[1256] Hassan, T., 'Nigeria: National Assembly to Install Full-Body Scanners', Daily Trust, 13th December 2011, http://allafrica.com/stories/printable/201112130281.html last visited 20/02/2012.
[1257] Ibid.

privacy implications and have raised peoples' concerns over their privacy not only in Africa but also elsewhere in the world (e.g. Europe and America).[1258]

Similar developments of databases have taken place in the context of population statistical data. In the last decade or so, population censuses in Africa have become computerized making it easy for access, sharing and distribution when required by governmental departments, private organizations or individuals who work in partnership with governments. Although censuses are very important in planning for development and making outreach programmes in different countries, they have not remained neutral with regard to privacy of individuals. The potential violations of privacy are expressed in the most oft-quoted German census decision of 1983 which partly annulled the Population Census Act on the ground of a fear of surveillance and feelings that such a statistical census was unjust invasion of privacy.[1259] These fears are no longer illusory in the wake of modern technologies. Neither are they limited to the Germans alone as correctly observed by Colin J. Bennett:-

> 'The factors that led to the enactment of Federal German Data Protection Act in 1977 were broadly the same as those in other countries-proposals for the establishment of large integrated databanks as well as unique PINs for administrative purposes. Anxieties about such developments should be seen against a background of higher rates of participation and a more acute sense of citizen efficacy within the German political culture.'[1260]

The most contested privacy issues with regard to population censuses in Africa are recorded in South Africa.[1261] Similarly, concerns for privacy emanating from population census have been felt in Kenya. The last population census in 2009 raised a number of questions including privacy. Undoubtedly, because of the post election violence of 2007 based on ethnic divisions and which took away the lives of many Kenyans, ethnical identification during the population census which came two years after the violence, was highly resisted. The question 'What tribe are you?' was the most controversial, in particular, given the recent memory of the 2007-2008 post-election

[1258] Banisar, note 1255, supra.
[1259] Note 2, supra; see also Hornung, G and Schnabel, C., 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination', Computer Law and Security Report, 2009, Vol.25, No.1, pp.84-88, at pp.84-85.
[1260] Bennett, p.75, note 1, supra.
[1261] For detailed discussion see chapter 6 of this thesis.

violence.[1262] The controversies surrounding ethnic identity in Kenyan census are well articulated in the responses of a Kenyan Peter Aling'o following an interview with Helen Nyambura-Mwaura, a Reuter's reporter in Nairobi:-

> 'We still have a lot of healing and reconciliation. We've begun to chest-thump around ethnicity again, not remembering that that was the problem in our elections. I don't think we have learnt our lessons as Kenyans, we are burying our heads in the sand.'[1263]

Yet, despite the local and international criticisms for inclusion of a question on one's ethnicity, the Kenyan government went ahead with its census while retaining the controversial question.[1264] In Ghana too, the 2010 population census saw increasing concerns for privacy. Some people dodged the census exercise thinking that when they were captured they would be squeezed to pay tax or their personal information could be subsequently used against them.[1265] The latter has been a growing common trend across African countries.

Somewhat linked to collection of vast amount of personal data in the databases are fraud and identity theft. The latter are also on the rise in many countries in Africa due to poor database security.[1266] At the same time, a lack of ID systems can have serious consequences for other rights.[1267] This has been the case with Nigeria where the Nigerian Central Bank announced recently that those without national identity cards will have a hard time getting bank loans.[1268]

- **Twitter and Facebook Revolutions**

There are heated debates whether the recent Arab uprisings in Tunisia and Egypt really deserve to be called 'Twitter Revolutions' and 'Facebook Revolutions'. Those who argue in favour of

---

[1262] Chrimes, S.B., 'Counting as Citizens: Recognition of the Nubians in the 2009 Kenyan Census', Ethnopolitics, 2011, Vol.10, No.2, pp.205-218, at p.206.
[1263] Reuters Africa., 'Ethnic Question in Kenya Census stokes Suspicions', 25th August 2009, http://af.reuters.com/article/topNews/idAFJOE57O0GP20090825 last visited 21/02/2012.
[1264] Chrimes, note 1262, supra; see also Huff Post World(internet newspaper)., 'Kenya Holds First Census In A Decade, Causes Outcry Over Ethnic Identity', posted on 24th August, 2009, http://www.huffingtonpost.com/2009/08/25/kenya-holds-first-census_n_268076.html?view=screen, last visited 21/02/2012; BBC News., 'Kenya begins contentious Census', 24th August 2009, http://news.bbc.co.uk/2/hi/8217637.stm last visited 21/02/2012.
[1265] Business and Gadget., '2010 Census for National Development (Ghana)', at http://www.qiam.org/news/2010-census-national-development-ghana last visited 21/02/2012.
[1266] Banisar, pp.126-127, note 1243.
[1267] Ibid.
[1268] Ibid.

these nomenclatures put consideration on the widespread use of user-generated content through the Twitter and Facebook social networks to plan and organize protests against regimes.[1269] Yet others have argued that calling uprisings in Tunisia and Egypt Twitter or Facebook revolutions overlooks ICT access in these countries.[1270] According to these commentators, in 2009 there were in Tunisia and Egypt only 34.1 and 24.3 Internet users per 100 inhabitants respectively.[1271] They argue that in Egypt only 7% of inhabitants are Facebook users, while 16% use the platform in Tunisia.[1272] This ICT penetration, at least according to these commentators, seem to suggest that the number of those connected to Twitter and Facebook was far disproportionate to the masses assembled in Tunis (Tunisia) and Tahrir Square in Cairo (Egypt), respectively. Similarly in further refuting claims for referring to the Arab spring in Tunisia and Egypt as 'Twitter Revolutions' and 'Facebook Revolutions', other commentators invented more appealing titles such as *The Great Twitter/Facebook Revolutions Fallacy.*[1273] Relying on similar statistics as above, these commentators have condemned the Western media and commentators alike for making unfounded propaganda appraising Twitter and Facebook as catalysts for revolution in the modern era.[1274] Yet, these arguments have been forcefully resisted by the pro-Twitter/Facebook Revolutions arguing that the democratic change in Islamic countries was/is conditional upon the use of communication technologies.[1275] These commentators argue that the low connectivity rates in these countries could/can not preclude communication technologies from reaching mass of enough audience.[1276] Through social communication technologies content is being distributed between networks of family and friends.[1277] While it is not the intention of this thesis to resolve these contested claims over what would be the appropriate name of the protests in Tunisia and Egypt, it is imperative to note that, the role of ICTs by both the protesters, to plan and organize protests as well as the regimes in crackdown is widely acknowledged by both rivals.[1278] The ICTs evolvement in the Arab spring is also acknowledged in case of the Libyan protests.

[1269] See e.g., 'Twitter and Facebook in the Arab Revolution' a post by David on Online Media Workshop, 22nd February 2011 at http://www.onlinemediaworkshops.com/blog/twitter-and-facebook-arab-revolution last visited 21/02/2012.

[1270] See e.g., Comninos, A., 'Twitter Revolutions and Cyber Crackdowns: User-Generated Content and Social Networking in the Arab Spring and Beyond', Association for Progressive Communications (APC), June 2011, pp.1-18, at p.5, http://www.apc.org/en/system/files/AlexComninos_MobileInternet.pdf last visited 20/02/2012.

[1271] Ibid.

[1272] Ibid.

[1273] The Politikal Blog., 'The Great Twitter/Facebook Revolutions Fallacy', 5th February 2011, http://mypolitikal.com/2011/02/05/the-great-twitterfacebook-revolution-fallacy/ last visited 20/02/2012.

[1274] Ibid.

[1275] Howard, P.N., The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam, Oxford University Press, Ney York, 2010, p.31 cited in Allagui, I., 'The Arab Spring and the Role of ICTs: Editorial Introduction', International Journal of Communication, 2011, Vol.5, pp.1435-1442, at p.1437.

[1276] Ibid.

[1277] Ibid.

[1278] See e.g., Comninos, pp.8-11, note 1270, supra.

In all the above cases, if anything, the Arab spring in the North Africa has demonstrated the clearest instances of violations of privacy by African governments through the use of modern technologies. First, the Tunisian, Egyptian and Libyan governments used advanced Internet filters to block content during the uprisings.[1279] In Tunisia, the government deployed a far more advanced technology in crackdown through stealing of user-names and passwords for Facebook, Twitter and online e-mail accounts like Gmail and Yahoo!.[1280] This was achieved through the injection of phishing scripts into the content of these pages before being sent to the end-user.[1281] The identification of users was soon followed by arrests, detentions and harassments of those involved in the creation and dissemination of user-generated content.[1282] Second, Twitter and Facebook were highly used as tools of state surveillance by security and state intelligences to identify and locate activists and protestors.[1283] Many people participating on Facebook pages were actually governments' agents or supporters of the regimes, spreading propaganda as well as spying on other facebook users.[1284] Third, the regimes especially those in Egypt and Libya also demonstrated their ultimate power over the Internet by virtually shutting down access to it[1285] or making interruptions frequently.

The Arab-style revolution in North Africa inspired protests across sub-Saharan Africa. Attempts of such revolutions were made in 2011 in Djibouti, Ivory Coast, Gabon, Malawi, Mozambique and Zimbabwe.[1286] Yet, these protests were not successfully due to various reasons which are beyond the analysis of this thesis. However it is noteworthy to mention that the '*Twitter/Facebook fallacy*' as some commentators have referred to it in an attempt to underplay the role of the social network technology in the Arab spring, was taken seriously by some of those regimes in sub-Saharan Africa. In Uganda, for example, President Yoweri Museveni after being declared a winner of the 2011 presidential election in what is believed to be a rigged election, the opposition coalition led by Kizza Besigye protested in Kampala (Uganda). However the protesters failed to amass in large numbers, as some commentators have suggested, a failure to totally tally its own results through its own SMS system as a result of interruption by the government.[1287] As a result,

[1279] Ibid, p.10.
[1280] Ibid.
[1281] Ibid.
[1282] Ibid.
[1283] Ibid.
[1284] Ibid.
[1285] Ibid, p.11.
[1286] Wikipedia, http://en.wikipedia.org/wiki/Impact_of_the_Arab_Spring last visited 22/02/2012.
[1287] Ibid.

the opposition coalition was unsure if it won the election or not. This had a negative impact in mobilization of protesters.

To sum up, the Twitter/Facebook revolutions have raised awareness to majority Africans over the privacy implications in interacting with social networks and other electronic communications variants. The possibilities to be identified when accessing or exchanging information or opinion, for example, and above all the potential possibilities of such communications to be intercepted or monitored with more advanced technology have raised more privacy concerns.

- **Fears**

Public fears over threats to privacy and related values have had significant contribution to the emergence and/or existence of data protection laws at least in Europe.[1288] One set of such fears related to increasing transparency, disorientation and disempowerment of data subjects *vis-à-vis data* controllers.[1289] Another set of fears concerned loss of control over technology. A third set pertained to human dehumanization of societal processes.[1290] Although it is doubtful if such fears have had significant impact in the emergence and/or existence of data protection laws in Africa, they have raised sufficient fears for privacy encroachments. Two sources of public fears come from government surveillance or reprisals and private sector's surveillance and unsolicited marketing practices. In the former case, fears for surveillance manifest through the extensive adoption of interception laws by most African governments including anti-terrorism legislation with interception law provisions. Uganda, for example, has recently adopted one of the most criticized wiretapping laws in Africa, the Regulation of Interception of Communication Act 2010. It had taken three years since 2007 for this law to be passed by the Ugandan legislature amid strong opposition from the members of parliament. However that opposition did not operate in the vacuum. It took into account the entire Ugandan political environment. This point is clearly summarized by Mayambala in the following paragraph:-

> 'Though the right to privacy in communication did not pose a major challenge in Uganda two decades ago, new developments in science and technology continue to pose new challenges to human rights, in particular the right to human dignity and privacy. In the fight against organized crime and terrorism,

[1288] Bygrave, p.107, note 24, supra.
[1289] Ibid.
[1290] Ibid.

> modern police and intelligence agencies are using information and surveillance technology, including phone tapping, that potentially affects numerous innocent citizens and constitutes far-reaching interference with the right to privacy. Lt. Gen. David Tinyefuza was possibly the first high profile government official to complain about phone tapping after his failed bid to resign from the army in 1997. In 2003, the Member of Parliament for Lira Municipality, Ms. Cecilia Ogwal, was up in arms with the government and President Yoweri Museveni in particular for allegedly tapping her mobile phone conversations. This was after the latter told Parliament on September 8, 2003, that he had listened in on a conversation between Ogwal and a rebel commander of the Lord's Resistance Army.'[1291]

In supporting the above view, Kaduuli posits:-

> 'The Ugandan Government is on the verge operationalizing official telephone tapping through the Regulation of Interception of Communication Bill 2007(already passed as law in 2010) and this has generated intense social, political, economic and legislative heat. Most Ugandans are concerned that their privacy will be infringed upon in the name of national security. Obviously, no individual feels comfortable knowing that there is a possibility of their (sic) phone being monitored.'[1292]

The most contentious area of the Ugandan interception law was and still is the authorization of interception. In the original Bill (2007) as it was introduced in the parliament this authority was placed in the designated Minister, an idea that was strongly rejected by the members of parliament.[1293] The latter preferred such mandate to be placed with a judge of the High Court of

---

[1291] Mayambala, p.6, note 38, supra.

[1292] Kaduuli, S.C., 'To Tap or Not to Tap? This is the Uganda Phone Question', WIRETAPPING: REGULATORY PERSPECTIVES, Ramakistaisah Jilla, ed., Hyderabad, India: Icfai University Press, 2010, pp.209-219, SSRN: http://ssrn.com/abstract=993545 last visited 22/02/2012; see also similar concerns for privacy raised by Bakibinga, note 61, supra who observes, 'Uganda is an emerging democracy and the political background reveals a history of turbulence and civil strife for many years, which resulted into the use of illegal means to gather intelligence(wiretapping without the sanction of court), which activities if not regulated, today can undermine the functioning of a democratic State.'

[1293] Outside Parliament, academics, practitioners, lawyers, local and international non-governmental organisations also raised alarm against the proposed interception law. See e.g., Amnesty International., 'Uganda: Amnesty International Concerns on the Regulation of Interception of Communications Bill, 2007', Amnesty International Publications, 2007, http://www.amnesty.org/en/library/asset/AFR59/005/2008/en/10bf8327-7507-11dd-8e5e-43ea85d15a69/afr590052008en.pdf last visited 22/02/2012.

Uganda. Although the final law came out with a victory on the side of the parliamentarians, still the scope of the authorization mandate is not clear especially the circumstances and purposes for such authorization by a judge.[1294]

In Zimbabwe the situation is totally horrible. Under the Zimbabwean Interception of Communications Act 2007 the designated Minister is vested with authority to issue a warrant of interception without any further intervention of a judge.[1295] Four categories of persons are allowed to lodge application for such warrant: the Chief of Defence Intelligence, the Director-General of the President's departments responsible for national security, the Commissioner for the Zimbabwe Republic Police and the Commissioner-General of the Zimbabwe Revenue Authority.[1296] Given Zimbabwe's poor human rights records, concerns for privacy of correspondence especially by the political opposition to President Robert Mugabe are very high.[1297] Explaining similar situation in Ghana, Branttie posits that because data related to SIM registration can be extrapolated to monitor calls and movements of subscribers via GPS data and locational signal traces and cell site triangulation, it is very effective tool to accurately track users.[1298] Accordingly, privacy of movement will be severely compromised by the national security operatives whose reputation for zealousness has already been known to cause very embarrassing national situations.[1299] In North Africa surveillance of citizens and monitoring of their electronic communications is commonplace.[1300] Yet, it is still early to predict if the Arab spring will improve the situation in future.

Surveillance and unsolicited communications for marketing from companies constitute another source of fears for privacy. Alongside these companies' surveillance, individuals also engage in

---

[1294] See e.g., Amnesty International., 'Uganda: Amnesty International Memorandum on the Regulation of Interception of Communications Act 2010', Amnesty International Publications, 2010, http://www.amnesty.org/en/library/asset/AFR59/016/2010/en/4144d548-bd2a-4fed-b5c6-993138c7e496/afr590162010en.pdf last visited 22/02/2012.

[1295] Zimbabwean Interception of Communications Act 2007, s.5.

[1296] Ibid.

[1297] See e.g., U.S Department of State., '2010 Human Rights Report : Zimbabwe',p.24, http://www.state.gov/documents/organization/160485.pdf last visited 22/02/2012; Human Rights Watch., 'World Report 2012: Zimbabwe Events of 2011', http://www.hrw.org/world-report-2012/world-report-2012-zimbabwe-0 last visited 22/02/2012.

[1298] Branttie, E., 'IMANI Report: The Failing SIM Card Registration Exercise- Millions of Dollars will be lost to the State. Ghana's Telecom Regulator MUST graduate SIM deactivation Exercise!', p.2, http://www.africanliberty.org/files/IMANI%20Report%20The%20Failing%20SIM%20Card%20Registration%20Exercise-%20Millions%20of%20Dollars%20will%20be%20lost%20to%20the%20State.%20Ghana%20Telecom%20Regulator%20MUST%20graduate%20SIM%20deactivation%20Exercise.pdf last visited 22/02/2012.

[1299] Ibid.

[1300] See e.g., Human Right Watch., 'The Internet in Mideast and North Africa: Free Expression and Censorship', Human Rights Watch 1999, http://www.hrw.org/sites/default/files/reports/midintnt996.PDF last visited 22/02/2012.

some minimum practices of surveillance and sending unsolicited communications. In either case the uses of CCTV at homes, offices, hotels and large shopping malls are now common in many places in Africa for purposes of preventing crimes. These technologies are supplemented by SMS text messages. All of these have generated fears of loss of privacy.[1301]

- **HIV/Aids**

Privacy in the context of HIV/Aids is, perhaps, the most notable area of rising privacy concerns in Africa. HIV/Aids plagued the African continent in 1980s. Since then it spread significantly. By 2010, it was estimated that Africa was by far the most continent hit by HIV/Aids. Reports reveal that by the end of 2010 an estimate of 22.9 million people were living with HIV in sub-Saharan Africa a figure which was equal to 68 per cent of the world population living with HIV by then.[1302] The epidemic had cost the lives of 1.3 million in the sub-continent by 2009 leaving 1.8 million as newly infected.[1303] Efforts to prevent or provide care and support to people living with HIV/Aids have raised a number of privacy law issues. Consent to HIV/Aids testing is the most controversial issue surrounding privacy. Many people in Africa are concerned with HIV/Aids testing without their consent. Since HIV/Aids has no prevention or cure, many people consider their health records in the context of HIV/Aids as most sensitive fearing stigmatisation.[1304] The second issue stemming from the first is about disclosure of HIV/Aids test results or status to third parties without authorisation of people concerned. For example, on 16 February 2012 the Star (a Kenyan newspaper) reported in one of its headlines, 'HIV Positive Girl sues paper over Disclosure of Her Status'.[1305] The basis of the claim was/is that the girl concerned was not asked her consent prior to such disclosure resulting into infringements of privacy and the right to dignity.

[1301] For detailed discussion see chapters 5,6 and 7 of this thesis.
[1302] UNAIDS., 'World AIDS Day Report 2011', p.7, http://www.unaids.org/en/media/unaids/contentassets/documents/unaidspublication/2011/JC2216_WorldAIDSday_report_2011_en.pdf last visited 23/02/2012.
[1303] UNAIDS., 'UNAIDS Report on the Global AIDS Epidemic', p.20, http://www.unaids.org/documents/20101123_GlobalReport_Chap2_em.pdf last visited 23/02/2012.
[1304] See e.g., Weiser, S.D *et al.*, 'Routine HIV Testing in Botswana: A Population-Based Study on Attitudes, Practices, and Human Rights Concens', PLoS Medicine, 2006, Vol.3, No.7, pp.1013-1022, at pp.1018-1019; Mbonu, N.C *et al.*, 'Stigma of People with HIV/AIDS in Sub-Saharan Africa: A Literature Review', Journal of Tropical Medicine, 2009, Article ID 145891, 14 pagesdoi:10.1155/2009/145891; Anglewicz, P and Chintsanya, J., 'Disclosure of HIV Status between Spouses in Rural Malawi', AIDS Care: Psychological and Sicio-Medical Aspects of AIDS/HIV, 2011, Vol.23, No.8, pp.998-1005, at p.1002.; The Wold Bank., Legal Aspects of HIV/AIDS: A Guide for Policy and Law Reform, The World Bank, Washington, D.C, U.S.A, 2007, http://siteresources.worldbank.org/INTHIVAIDS/Resources/375798-1103037153392/LegalAspectsOfHIVAIDS.pdf last visited 23/02/2012.
[1305] The Star, 16th February 2012, http://www.the-star.co.ke/national/national/62763-hiv-positive-girl-sues-paper-over-disclosure-of-her-status last visited 23/02/2012.

Disclosure has also resulted into serious problems in the healthy and employment sectors. Medical practitioners in Africa claim to be in dilemma to disclose or not to disclose HIV/Aids status to a victim's sex partner or relatives as the case may be.[1306] Yet, in some cases without any consent from a concerned person, they have secretly communicated HIV/Aids test results directly to employers while bypassing the employees who were the subject of testing.[1307] Somewhat linked with the disclosure issue, is discrimination of people living with HIV/Aids. Once their HIV/Aids status is revealed, many people living with HIV/Aids have found themselves discriminated. This discrimination does not just end with the employment sector which is commonly cited by commentators[1308] but extends to other spheres of life. For example, in Kenya, discrimination has also manifested in issues of land ownership.[1309]

In response to the above concerns, some governments as well as private sector institutions in Africa have developed policies as well as special legislation. Tanzania, Kenya, Uganda, Namibia, South Africa serve as examples. However, the major weakness of these laws and policies is that they focus on issues of confidentiality alone rather than privacy. Admittedly, while confidentiality is an aspect of privacy, confidentiality as such is inadequate to protect health records in the context of HIV/Aids. Apart from that, many of the laws are vague in terms of scope and ambit. Nevertheless in relative terms, concerns for privacy in the context of HIV/Aids in Africa has manifested through development of a lager corpus of case law on privacy.[1310] Although such case law still falls short of the principles of data privacy it serves to demonstrate how far Africans put significant weight on privacy of their health records.

[1306] See e.g., Vu, L *et al.*, 'Disclosure of HIV Status to Sex Partners Among HIV-Infected Men and Women in Cape Town, South Africa', AIDS Behav, 2012, Vol.16, No.1, pp.132-138.

[1307] Makulilo, pp.573-575, note 224, supra.

[1308] See e.g., Dwasi, J.A., The Human Right to Work in the Era of HIV and AIDS, Law Africa, Nairobi/Dar es Salaam/Uganda, 2009; Makulilo, note 224, supra.

[1309] Aliber, M and Walker, C., 'The Impact of HIV/AIDS on Land Rights: Perspectives from Kenya', World Development, 2006, Vol.34, No.4, pp.704-727.

[1310] For a detailed review of case law on HIV/Aids in African jurisdictions see e.g., Ladan, M.T., 'The Role of Law in the HIV/AIDS Policy:-Trend of Case Law in Nigeria and Other Jurisdictions', Inaugural Lecture delivered at the Ahmadu Bello University, Zaria, Nigeria, 2008, pp.1-64, at pp.19-22; Tadesse, M.A., 'HIV Testing from an African Human Rights System Perspective: An Analysis of the Legal and Policy Framework of Botswana, Ethiopia and Uganda', LL.M Thesis, University of Pretoria, South Africa, 2007; also further discussion on HIV/Aids is given in chapters 6 and 7 of this thesis.

- **Traumas of Past Injustice**

The concepts of justice and injustice have been a subject of philosophical debates for centuries since the Plato's *Republic*.[1311] These debates are not covered here because of little bearing to the issues addressed. Yet, it is sufficient to point out that an unjust system presupposes existence of oppression, exploitation, repression, inhibition or restraints whether at an individual or group level or by the state. In Africa the most widely cited traumas of past injustice are those relating to the system of apartheid in South Africa and the Rwandan Genocide.[1312] However, while these are commonly cited examples of past injustice due to the magnitude of their effects, there are other past injustices in Africa. For example, the dictatorship of military rulers in Africa qualifies in the definition given above. Be as it may, commentators are in agreement that privacy concerns are nourished by certain concrete experiences such as the traumas of fascist oppression prior to and during World War Two.[1313] Banisar argues that one of the reasons for adopting privacy laws in many countries including South Africa (which has not yet adopted omnibus data protection legislation) is to remedy privacy violations that occurred under previous regimes and prevent those abuses from occurring again.[1314]

- **E-Commerce**

E-commerce in Africa is still evolving. Its current low level is a result of inadequate e-commerce infrastructure. Yet, where it has started to develop consumer trust and confidence; cyber-crimes and identity thefts have raised serious concerns. This is largely because e-commerce transactions collect vast amount of personal information. The 'Nigerian Advance Fee Scam' is the most popularly feared across Africa and even beyond. And, has caused a lot of privacy concerns in online commercial transactions. Suffice here to quote one example:-

'Lagos, Nigeria.

[1311] See e.g., Sachs, D., 'A Fallacy in Plato's Republic', The Philosophical Review, 1963, Vol.72, No.2, pp.141-158; Rawls, J., 'Justice as Fairness', The Philosophical Review, 1958, Vol.62, No.2, pp.164-194; McBride, W.L., 'The Concept of Justice in Max, Engels, and Others', Ethics, 1975, Vol.85, No.3, pp.204-2018; Rawls, J., A Theory of Justice, Revised Edition, Harvard University Press, 1971.

[1312] See e.g., Weldon, G., 'A Comparative Study of the Construction of Memory and Identity in the Curriculum of Post-Conflict Societies: Rwanda and South Africa', International Journal of Historical Learning, Teaching and Research, 2003, Vol.3, No.2, pp.55-72, at p.55; King, R.U., 'Healing Psychological Trauma in the Midst of Truth Commission: The Case of *Gacaca* in Post-Genocide Rwanda, University of Toronto Press Journals, 2011, Vol.6, No.2, pp.134-151. Further discussion on South African Apartheid is given in chapter 6 of this thesis.

[1313] Bygrave, p.108, note 24, supra.

[1314] Banisar, D., 'Privacy and Data Protection Around the World', Conference Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13th September 1999, pp.1-5, at p.2, http://www.pcpd.org.hk/english/infocentre/conference.html last visited 23/02/2012.

Attention: the President/CEO

Dear Sir,

Confidential Business Proposal

Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers of Commerce and Industry, I have the privilege to request for your assistance to transfer the sum of $47,500,000.00 (forty seven million, five hundred thousand United States dollars) into your accounts. The above sum resulted from an over-invoiced contract, executed commissioned and paid for about five years (5) ago by a foreign contractor. This action was however intentional and since then the fund has been in a suspense account at the Central Bank of Nigeria apex bank.

We are now ready to transfer the fund overseas and that is where you come in. It is important to inform you that as civil servants, we are forbidden to operate a foreign account; that is why we require your assistance. The total sum will be shared as follows: 70% for us, 25% for you and 5% for local and international expenses incident to the transfer.

The transfer is risk free on both sides. I am an accountant with the Nigerian National Petroleum Corporation (NNPC). If you find this proposal acceptable, we shall require the following documents:-

(a) your banker's name, telephone, account and fax numbers.
(b)your private telephone and fax numbers- for confidentiality and easy communication.
(c) your letter-headed paper stamped and signed.

Alternatively we will furnish you with the text of what to type into your letter-headed paper, along with a breakdown explaining, comprehensively what we require of you. The business will take us thirty (30) working days to accomplish.

Please reply urgently.

Best regards'[1315]

[1315] Scambusters.org., 'About the Nigerian Scam(Nigeria Advanced Fee Scam): Internet ScaBuster#11', http://www.scambusters.org/NigerianFee.html last visited 1/03/2012.

The above letter seeks to collect personal information for purposes of commission of fraud. It is estimated that the Nigerian Crimes Division of the Secret Service receives approximately 100 telephone calls from victims or potential victims of advanced fee scam and about 300-500 pieces of related correspondence per day about it.[1316]

- **World Summit on the Information Society-Tunis 2005**

The World Summit on the Information Society (WSIS) was a pair of United Nations-sponsored conferences about information, communication and, in broad terms, the information society that took place in 2003 in Geneva and in 2005 in Tunis.[1317] One of its chief aims was to bridge the so-called global digital divide separating rich countries from poor countries by spreading access to the Internet in the developing world.[1318] One of the principles of the WSIS in Geneva of 2003 states:-

> '58. The use of ICTs and content creation should respect human rights and fundamental freedom of others, including personal privacy, conscience, and religion in conformity with relevant international instruments.'[1319]

Reaffirming the Geneva vision from an African perspective during the WSIS in Tunis (on 16 November 2005), the former President of South Africa, Mr. Thabo Mbeki made the following statement:-

> 'Our country and continent are determined to do everything possible to achieve their renewal and development, defeating the twin scourges of poverty and underdevelopment. In this regard, we have fully recognised the critical importance of modern ICTs as a powerful ally we have to mobilize, as reflected both in our national initiatives and the priority programmes of NEPAD, the New Partnership for Africa's Development. We are therefore determined to do everything we can to implement the outcomes of this World Summit on the Information Society and appeal to all stakeholders similarly to

[1316] Ibid.
[1317] Wikipedia, http://en.wikipedia.org/wiki/World_Summit_on_the_Information_Society last visited 1/03/2012.
[1318] Ibid.
[1319] Geneva Declaration of Principles 2003, Principle 58, Document WSIS-03/GENEVA/DOC/4-E 12 December 2003, http://www.itu.int/wsis/docs/geneva/official/dop.html last visited 1/03/2012.

commit themselves to take action to translate the shared vision of an inclusive development-oriented information society in practical reality.'[1320]

The significance of the WSIS cannot be over exaggerated. While it did not produce directly its effects over the people, it inspired African governments to commit themselves in using ICTs in their development efforts. This also meant that the African governments had/have to develop policies and regulations on ICTs. To ensure that these commitments are made a reality, WSIS has established a monitoring procedure which periodically make follow-up on performance from a country to regional organisation level.[1321]

- **International, Regional and National Data Protection Laws**

International, regional and national policies and codes for protection of privacy have had impact on privacy in Africa. However in relative terms, regional policies and codes have been more instrumental in influencing concerns for privacy in Africa and consequently adoption of recent comprehensive data privacy legislation more than the others. Yet, both international and regional data privacy law *vis-à-vis* the national legal systems in Africa are subject to the theories of dualism and monism.[1322] The former treats international law as distinct from domestic legal order, meaning that the application of the former in the latter depends on the process of incorporation. Hence ratification of a treaty by a state is one thing and its incorporation is yet another. Under dualism the national legal order is superior to international law. In contrast, the monist theory makes international law part and parcel of the national legal order and accordingly self-executing.

Yet under dualism, where international law has either not been ratified or ratified, but still not incorporated, there is increasingly tendency of lawyers and judges using it to interpret domestic legislation.[1323] In certain cases, international law offers inspiration for development of particular

---

[1320] Capurro, R., 'Information Ethics for and from Africa', International Review of Information Ethics, 2007, Vol.7, No.9, pp.1-13, at p. 2.

[1321] See e.g., ITU., 'WSIS Forum 2011: Outcome Document', http://www.itu.int/wsis/implementation/2011/forum/inc/Documents/WSISForum2011OutcomeDocument.pdf

[1322] For detailed analysis of dualism and monism in relation to Africa, see e.g., Oppong, R.F., 'Re-Examining International Law: An Examination of Recent Trends in the Reception of International Law into Legal Systems in Africa', Fordham International Law Journal, 2007, Vol.30, No.2, pp.296-345.

[1323] See e.g., Layton, R., 'When and How Can Domestic Judges and Lawyers use International Law in Dualist Systems', http://training.itcilo.org/ils/cd_use_int_law_web/additional/Library/Doctrine/Dualist%20Systems_Layton.pdf last visited 28/02/2012; Quansah, E.K., 'An Examination of the Use of International Law as Interpretative Tool in Human Rights Litigation in Ghana and Botswana', in Killander, M(ed)., International Law and Domestic Human rights Litigation in Africa, Pretoria University Law Press(PULP), South Africa, 2010, pp.37-56. Tanoh, A and

domestic legislation or decision making process.[1324] In Africa, countries with common law legal system (i.e. former British colonies), practise dualism. This is with the exception of Namibia and Kenya which, though follow the English legal system, have maintained monist practice similar to the countries which follow the continental legal system.[1325] In this way, the African approach towards international law has to be considered whenever assessing the influence of international and regional law in their data privacy legislative development.

At international level, three instruments can be identified which relate to protection of the right to privacy: the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the *UN Guidelines* with regard to the protection of personal data.[1326] Since these are UN's instruments, they apply to African countries by virtue of being members to the United Nations. As pointed out in previous sections of this thesis the Bill of Rights in many African national constitutions have their foundation in the UDCHR as well as ICCPR. The right to protection of privacy is one of the clauses enshrined in such Bill of Rights. However their impact in shaping privacy ideas and consciousness as well as adoption of policies and regulation has not been much significant. This is partly because such Bill of Rights became part of the African legal system through independence constitution which initially received a negative attitude and response from African nationalist elites. Even after their re-appearance in African constitutions in 1980s and 1990s, African leaders have rendered them impracticable in practice. Sometimes the general political environment is made to work negatively to the Bill of Rights as is the case with Zimbabwe or the Bill of Rights themselves are formulated with numerous clawback clauses rendering them no longer important. Also important to note is that in some African countries those international instruments have no direct application. They have to be incorporated, especially in dualist states, in order to take effect. This allowance gives these countries great leeway to maneuver the application of the Bill of Rights. Yet, in some monist states, international law has been disregarded.[1327] Nonetheless, the UDHR and ICCR are increasingly becoming important as they provide the normative basis for the right to privacy in Africa. In contrast to the UDHR and ICCR, the *UN Guidelines* (the only data protection code

---

Adjolohoum, H., 'International Law and Human rights litigation in Côte d'Ivoire and Benin', Killander, M(ed)., International Law and Domestic Human rights Litigation in Africa, Pretoria University Law Press(PULP), South Africa, 2010, pp.109-120.

[1324] Ibid.

[1325] See e.g., Tanoh, A and Adjolohoum, H., 'International Law and Human rights litigation in Côte d'Ivoire and Benin', Killander, M(ed)., International Law and Domestic Human rights Litigation in Africa, Pretoria University Law Press (PULP), South Africa, 2010, pp.109-120; Ndayikengurukiye, M., 'The International Human Rights Law as a source of Law in the Burundian Judicial System', LL.M Dissertation, University of Makerere, Uganda, 2005.

[1326] See a comprehensive review of these instruments in para 3.2 of this thesis.

[1327] See e.g., Tanoh, and Adjolohoum, pp. 114-115, note 1325, supra; Ndayikengurukiye, pp.21-22, note 1325.

under the United Nations' umbrella) has not generally yielded any significant influence for the right to privacy in Africa. As alluded to, these *Guidelines* are not binding. They are there only to provide guidance for such UN members or organizations in member states to use whenever they develop data protection policies and regulations. Also important, the fact that they were preceded by some national and regional data privacy policies and regulations, especially in Europe, which have had influence beyond their area and limits of operation, have rendered the former less influential.

The only regional policy and code for privacy and data protection outside of Africa which has been influential in matters of privacy in the continent is Directive 95/46/EC. It is imperative to mention that the Council of Europe Convention 108 with regard to automatic processing of personal data is the only European regional treaty open for accession by non-European states. Yet, currently this Convention is not open to African countries for accession.[1328] As it has been the case elsewhere, Directive 95/46/EC has generated both political and economic pressure over African countries to adopt data privacy laws in the European-style. Article 25 of Directive 95/46/EC clearly says that transfer of personal data to third counties will only be allowed if such countries maintain an adequate level of data protection law similar to the Directive. Nevertheless some exceptions for transfer of such personal data from Europe to third countries are permitted under Article 26 of the Directive.

Unlike the international law under the auspices of the United Nations, Directive 95/46/EC is the European Union law. It binds upon its member states only and those under the European Economic Area. Since African countries are not members of the EU or EEA, they are not under any obligation to comply with the requirements of the Directive. However there are exceptions. As pointed out, Article 25 requires any non-EU/EEA member state wishing to receive personal information of citizens in such regions must have a system of privacy protection that satisfies the 'adequacy' standard under the European Directive. African countries are subject to this clause. Yet, since the above European law came into force in 1998, there is no African country which has been declared as providing 'adequate' level of protection of personal data. In 2010 some African countries which have implemented comprehensive data privacy law applied to the EU for accreditation as satisfying this level of protection. In this list there are the following countries: Mauritius, Burkina Faso, Tunisia and Morocco. While the reports for the rest of these countries have not been made public that of Tunisia is publicly available. As already pointed out, the first

[1328] Explanatory Report, note 701, supra.

report with regard to Tunisia data privacy law stated clearly that Tunisia's regime is not adequate. It is also suggested that the other reports for the rest countries may likely not be positive, suggesting why they are kept confidential. These reports do not either end the matter. As said, Article 26 provides exceptions to the general rule laid down in Article 25, making it not absolute. No doubt, these exceptions were made in realization of the difficulty to satisfy the 'adequacy' standard. Although at the risk of generalization, logic dictates that since no African country has been declared to provide 'adequate' level of data protection, the current continued flow of personal data from Europe to Africa is justified at least under one or more criteria set out in article 26 of the Directive. Admittedly, these criteria are limited in their application and consequently are likely to affect the volume of personal data from Europe to Africa.

In relation to the volume of personal data in the preceding paragraph, the prevailing view is that Africa needs to satisfy the requirements of the European Directive in order to attract investment and outsourcing industries. These economic justifications manifest in literature (journal articles, commentaries, reference books, newspapers, magazines, reports), legislation, Bills, policies, hansards, treaties and conventions as well as in *travaux préparatoires*. Protection of individual personal data of citizens and/or residents in African countries is usually secondary. Some examples illustrating the dominant justification for adoption of data privacy legislation need to be mentioned. For example, in 2004 Bygrave maintained that the interest in legislating data privacy legislation in Africa was due to the impact of Articles 25 and 26 of Directive 95/46/EC and the desire by African countries to meet the requirement of the European law set in those provisions.[1329] Although Bygrave did not clearly indicate the motivation for such desire, in 2010 he made clearly the point that African countries adopted data privacy law in EU-style in order to safeguard their outsourcing industry pointing examples of Tunisia and Morocco.[1330] Beyond these economic justifications, Bygrave mentions traumas from relatively recent first hand-experience referring to South Africa's apartheid experience as justification for development of data privacy law.[1331] The economic justification put forward by Bygrave is repeated by other commentators such as Kusamotu,[1332] Ncube,[1333] Gayrel,[1334] ARTICLE 19,[1335] Enyew[1336] and Traca

[1329] Bygrave, note 51, supra.
[1330] Bygrave, note 56, supra.
[1331] Ibid; see also Bygrave, note 1318, supra.
[1332] Kusamotu, pp.157-158, note 38, supra.
[1333] Ncube, notes 172, 173 and 174, supra.
[1334] Gayrel, p.18, note 38, supra; see also, Gayrel, C., 'Mauritius: Data Protection in an Evolving Island Economy', Privacy Laws & Business International Report, 2011, No.114, pp.20-22.
[1335]ARTICLE 19., 'Kenya: Draft Data Protection Bill critically limited', Statement issued on 7 November 2011, http://www.article19.org/resources.php/resource/2825/en/kenya:-draft-data-protection-bill-critically-limited last visited 14/03/2012.

and Embry.[1337] In this list Enyew, Kusamotu, Traca and Embry and ARTICLE 19 make clearer the economic justification theory. In the context of Ethiopia, Enyew argues:-

> 'Turning to Ethiopia, the country is not an exception. The country is required to satisfy the adequate level for transfer of personal data from Europe. Ethiopia has, wants to have extensive trade relations with European countries as well as other foreign countries. It has also attempted to privatize many sectors so that foreign investors can participate in the economy. The existence of appropriate and efficient law is important to regulate and promote investment. So long as the Ethiopian law is found to lack of adequate protection of privacy, it will encounter limits on the transfers of personal information. Limitations on the flow of personal information discourage investment and commerce. Beyond trans-border data flow, the enactment of privacy law is equally important to put the legal framework in place for e-commerce within the country. Thus, the enactment of privacy law is very essential to facilitate e-commerce (which the country will introduce it in the future), international trade and investment.'[1338]

Somewhat similar to the above paragraph, but slightly different, Kusamotu identifies who will be behind the introduction of data privacy legislation in Nigeria. He posits, as for Nigeria, drives to introduce EU-compatibility law within Nigeria would come from the business community, and not the general public.[1339] In the same vein Traca and Embry posit that 'while the Angolan Data Protection Act 2011 may have been enacted by the National Assembly as an instrument through which inalienable human rights could be enshrined in this particular context, the Angolan legislator took time and care in framing the statute so as to incorporate a healthy respect for the needs of business to conduct their operations as swiftly and as smoothly as possible. This Act is very much a reflection of contemporary Angola, following on from several other legislative reforms at a time when business in Angola is growing at an increasingly fast pace, with no sign of slowing down anytime soon.'[1340]

[1336] Enyew, A.B., 'Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia', LL.M Thesis, University of Oslo, Norway, 2009.
[1337] Traca and Embry, p.40, note 38, supra.
[1338] Enyew, pp.47-48, note 1336, supra.
[1339] Kusamotu, p.157, note 38, supra.
[1340] Traca and Embry, note 1337, supra.

In criticizing the narrow scope of the Kenyan draft Data Protection Bill 2009 in the context of the economic justification theory, the ARTICLE 19 posits:-

> 'While the draft will bring greater accountability to the processing of information about Kenyan citizens held by government bodies, the restriction to public bodies substantially limits the usefulness of the act as a means to enhance international trade to Kenya. European (and many other countries') law limits the transfer of personal information for outsourcing and other reasons to only countries with adequate data protection laws, which is why many countries in Africa, Asia and Latin America have adopted laws recently. This bill as drafted will not allow European data controllers to transfer personal information to Kenya because it does not apply to private sector. Thus a major reason for adopting the bill will not be achieved.' [1341]

Noteworthy, the economic justification behind the adoption of data privacy legislation in Africa has also manifested in the reports for analysis of the adequacy of protection of personal data in some African countries.[1342] Similarly, the justification was prominent in the parliamentary discussions in Mauritius and is currently featuring in South African legislative process.[1343] As pointed out, there is currently no general survey to concretize the extent to which African countries have economically been affected by the restriction on transfer of personal data from Europe. In most cases such claims have been made by sweeping statements. However on country level, Morocco seems to have undertaken a study on the impacts of European data privacy law. In 2008, a report by the Moroccan Ministry of economy pointed out that the low volume of relocation of banking and insurance services to Morocco was partly due to a lack of protection of personal data transferred to the Kingdom, and recommended the adoption of legislation of this subject, which followed in 2009.[1344]

Apart from the economic aspect of Articles 25 and 26 of the Directive 95/46/EC considered above, there is also its political dimension. The latter rests upon the sovereignty of the state. After attainment of political independence in 1960s and 1970s, African countries became

[1341] ARTICLE 19, note 1335, supra.
[1342] See e.g., CRID, p.7, note 899, supra.
[1343] Further details are provided in chapters 5 and 6 of this thesis.
[1344] Ministère de l'Economie et des Finances, Dé loc a l i s a t ion de s a c t i v i t é s de s e r v i c e s au Ma roc, Et a t de s l i eux e t oppor tuni t é s Juillet 2008, p.15,
http://www.finances.gov.ma/depf/publications/en_catalogue/etudes/2008/delocalisation.pdf
last visited 29/02/2012; also cited in Gayrel, note 1334, supra.

autonomous sovereign states. Accordingly, a provision requiring third countries, in this case African countries, to enact legislation in compliance to European law, is practically interfering with their sovereignty. This is despite the fact that finally it is African national legislative bodies which are the ones to pass the legislation. Hobby posits that when considered in a broad context, it is hard to avoid the feeling that the EU's implementation of such a wide sweeping regulatory exercise in the realm of fundamental rights goes far by effectively creating a worldwide data privacy regime utilizing the proverbial back door.[1345] Although this argument has not yet featured more seriously in the emerging African scholarship, grounds for its emergence already exist. Firstly, it is due to the apprehension by the Article 29 Data Protection Working Party (the EU body which gives its opinion to the EU Commission as to the adequacy level of protection of legislation in third countries) that the act of engaging in assessment of legal systems of sovereign independent states may result into political provocation particularly where such systems fail to meet the adequacy standard under the European law.[1346] Secondly, is the negative feeling by African countries, that a foreign legal order has been imposed upon them just like it was the case under the colonial rule. The latter resulted into transplantation of the present day civil and common law legal systems in Africa.[1347] Accordingly, the level of its acceptability and compliance by local population becomes negatively affected.

However, the political dimension of Articles 25 and 26 of Directive 95/46/EC should not be exaggerated. This is because calls by scholars within their countries in Africa to their respective governments, to enact data privacy legislation, have rarely raised any caution as to the imposition of the European law on Africa. This is partly because legal transplantation in Africa is not a new phenomenon. In fact, the civil and common law legal systems which were imposed during colonial rule by force have so far brought benefits in Africa after independence. This, to some greater extent, may have undermined concerns for regarding European law as imposed in Africa. Also important to take into account, as African countries increasingly become part of regional or international bodies, the influence of foreign law is felt quite often. Moreover, in the course of judicial interpretation judges and lawyers rely frequently on foreign case law to interpret local

[1345] Hobby, pp.157-158, note 1048, supra.
[1346] Article 29 Data Protection Working Party, notes 892 and 893, supra.
[1347] See e.g., Ferreira, C., 'The Europeanization of Law' in Oliveira, J and Cardinal, P(eds)., One Country, Two Systems, Three Legal Orders-Perspective of Evolution: Essays on Macau's Autonomy after the Resumption of Sovereignty by China, Springer-Verlag, Berlin/Heidelberg, 2009, pp.171-190, at p.184; Mancuso, S., 'Legal Transplants and Economic Development: Civil Law vs. Common Law?' in Oliveira, J and Cardinal, P(eds)., One Country, Two Systems, Three Legal Orders-Perspective of Evolution: Essays on Macau's Autonomy after the Resumption of Sovereignty by China, Springer-Verlag, Berlin/Heidelberg, 2009, pp.75-90.

legislation, especially where no case law by superior courts in Africa exists. This has in turn accelerated the borrowing and permeation of foreign law in African countries.

Before concluding thia part, one fallacy by some African states has to be cleared. Some African countries (e.g., Cape Verde, Angola, Francophone Africa, Mauritius, etc) with data privacy legislation claim their legislation to be influenced by national laws of particular EU member states. Admittedly, while they are some variations in national data privacy law of EU member states, it is imperative to note that the effect of national data privacy law by an EU member country to Africa is practically the same as the Directive itself. This is because, in the first place, each EU member country is required to transpose the European Directive under its national legal system. Through this process, EU law becomes part of the legal system of its member states. Moreover, and as it has been pointed out, the national data protection authorities in EU member states have significant role in determining the adequacy level in third countries, particularly on specific transfers. In this regard, any assessment by a data protection authority affects other member states in some ways. This is further solidified by the fact that a notification for this kind of assessment has to be communicated to all member states in the EU.

Regional/sub-regional data privacy agreements and national legislation within Africa (see 4.4) may have some influence too in rising privacy concerns and legislation within their jurisdictions and in some other African countries. These legal instruments, after they had received initial push from the European law, have also imposed the adequacy standard against transfer of personal data to foreign countries including fellow African countries. The latter either fall within or outside the regional/sub-regional arrangements with data privacy law or without data privacy legislation. This point is well demonstrated by the following provisions of the African regional, sub-regional and national laws of African countries with data privacy legislation:-

AU Cyber Convention, Art II-41:-

> 'The data processing official shall not transfer personal data to a non-Member State of the African Union unless such a State offers sufficient level of protection of the private life, freedoms and fundamental rights of persons whose data are being or are likely to be processed.

Before any personal data is transferred to the said third country, the data processing official shall give prior notice of such transfer to the protection authority.'[1348]

ECOWAS, Art 36:-

'(1) The data controller shall transfer personal data to a non-member ECOWAS country only where such a country provides an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data.

2) The data controller shall inform the Data Protection Authority prior to any transfer of personal data to such a third country.'[1349]

SADC, Art 48(1):-

'Personal data shall only be transferred to recipients, other than member states of the SADC, which are not subject to national law adopted pursuant to this model-law, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out.'[1350]

Angola, Section 33:-

'The international data transfer is only possible subject to notification to the Data Protection Agency and to countries which ensure an adequate level of protection.

A country is considered to ensure an adequate level of protection when it guarantees, at least a level of protection equal to that established in this law.

[1348] AU, Cyber Convention 2011, Art II-41, note 1395, infra.
[1349] ECOWAS, Supplementary Act 2010, Art 36, note 1398, infra.
[1350] SADC, Data Protection Model-Law 2012, Art 48(1), note 1478, infra.

The Data Protection Agency shall decide whether a foreign country ensures an adequate level of protection through the issuance of an opinion.

The adequacy of data protection in a foreign country shall be assessed by the Data Protection Agency on the basis of all circumstances surrounding a data transfer, especially given the nature of the data, the purpose and duration of the proposed processing operation, the countries of final destination and rules of law, whether general or sectoral, in force in that country including the professional rules and security measures which are complied with in that country.'[1351]

Benin, Section 9:-

'The data controller shall not transfer any personal data abroad unless the foreign country provides a sufficient level of protection for privacy rights and the rights and freedoms of data subjects in relation to the processing of personal data.

The level of protection provided by the country shall be assessed in light of data protection laws and security measures that are applied in the foreign country, such as for the purpose, duration, nature, origin and the intended destination of the personal data.'[1352]

Burkina Faso, Section 24:-

'The transfer of personal data from the territory of Burkina Faso abroad, which is subject to automatic processing as prescribed by Article 19, is possible only if it complies with the requirements of this Act. However, in exceptional circumstances, a transfer may be authorized by decree with the approval of the DPA.'[1353]

[1351] Angola, Lei nº 22/11 Da Protecçao de Dados Pessoais 2011, s.33.
[1352] Benin, Loi n° 2009-09 du Mai 2009 Portant Protection des Données à Caractère Personnel 2009, s.9.
[1353] Burkina Faso, Loi n° 010-2004/AN Portant Protection des Données à Caractère Personnel 2004, s.24.

Cape Verde, Section 19:-

> 'Notwithstanding the provisions of this Act and other relevant legislation on protection personal data, the transfer of personal data abroad can only take place with respect to the provisions of this law and in particular if such country ensures an adequate level of protection.
>
> The adequacy of protection shall be assessed in the light of all circumstances surrounding a transfer, in particular the nature of the data, the purpose and duration of the proposed processing operation, countries of origin and final destination, the rules of law, both general and sectoral in force in the country concerned, as well as the professional rules and security measures that are complied with in that country.'[1354]

Mauritius, Section 31:-

> (1) Subject to subsection (2), no data controller shall, except with the written authorization of the Commissioner, transfer personal data to a third country.
>
> (2) The Eighth data protection principle specified in the First Schedule shall not apply where-
>
> (c) The transfer is made on such terms as may be approved by the Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subjects.
>
> (3) For the purpose of subsection (2) (c), the adequacy of the level of protection of a country shall be assessed in the light of all the circumstances surrounding the data transfer…'[1355]

[1354] Cape Verde, Lei nº 133/V/2001, de 22 de Janeiro Regime Jurídico Geral de Protecção de Dados Pessoais a Pessoas Singulares 2001, s.19.
[1355] Mauritius, Data Protection Act No.13 of 2004, s.31.

Morocco, Section 43:-

> 'The data controller shall not transfer any personal data to a foreign country unless that country ensures a sufficient level of protection for privacy rights and freedoms.
>
> The level of protection provided by the foreign country shall be assessed in light of the regulations and security measures applicable in that country, the characteristics of the processing such as the purpose, duration, nature, origin and intended destination of personal data.
>
> The DPA has established a list of countries that comply with the provisions mentioned above.'[1356]

Senegal, Section 49:-

> 'The data controller shall not transfer any personal data abroad unless the foreign country ensures a sufficient level of protection for privacy rights, rights and freedoms of data subjects in relation to the processing of personal data. Before any transfer of personal data to a foreign country, the data controller shall inform the DPA.'[1357]

Tunisia, Sections 51 and 52:-

> 'The transfer of personal data to a foreign country is prohibited when it may endanger public security or Tunisia's vital interests.
>
> The transfer of personal data to a foreign country for the purpose of processing or for the future purpose of processing is not permitted if the country does not provide an adequate level of protection. The adequacy level of protection shall be assessed in light of the nature, purpose for which and period during which the personal data are intended to be processed; where the

[1356] Morocco, Loi n° 09-08 Relative à la Protection des Personnes Physiques à l'égard du Traitement des Données à Caractère Personnel 2009, s.43.
[1357] Senegal, Loi n° 2008-12 sur la Protection des Données à Caractère Personnel 2008, s.49.

data shall be transferred to; and the security measures taken to ensure the safety of the personal data. In any case, the transfer of personal data must be carried out in accordance with the provisions of the Act.'[1358]

In Seychelles, sections 8(3) (e), 9(2) (e) 16(1), 45(1), (5) and (6) of the Seychelles' Data Protection Act No. 9 of 2003 imply that data may not freely be transferred from Seychelles to a foreign country. This prohibition, although does not clearly use the language of 'adequate level of protection', appears to be the standard intended to be used for determining if a transfer of personal data to a foreign country will receive protection similar to what the Seychelles data privacy law provides.

Accordingly, African countries have placed themselves in a similar position as the European Union for assessing the adequacy standard of laws in other African jurisdictions. Linked to the previous discussion and analyses, this reason has partly silenced concerns for imposition of European law in Africa because the same claims against the European Directive would have delegitimized the adequacy clauses in African data privacy laws to their fellow African countries.

4.3.1.2 Negative Determinants

- **Lack of Awareness of Privacy Risks**

Privacy awareness reflects the extent to which an individual is informed about privacy practices and policies, about how disclosed information is used, and is cognizant about their impact over the individual's ability to preserve her private space.[1359] Lack of privacy awareness is perhaps one of the most negative determinants that have impeded the growth of privacy concerns in Africa and consequently affecting the adoption of privacy policies and legislation. Understandably this lack of individuals' awareness of privacy risks partly reflects the value individuals attach on privacy of their personal information. Sometimes privacy policies and legislation may exist in African countries however their ignorance by individuals produce the same result. Froomkin summaries the condition in which an individual's lack of awareness affects the value he or she

[1358] Tunisia, Loi n° 2004-63 Portant sur la Protection des Données à Caractère Personnel 2004, ss. 51 and 52.
[1359] Xu, H *et al.*, 'Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View', International Conference on Information Systems (ICIS) Proceedings, 2008, pp.1-16, at 6.

attaches on privacy in his famous expression 'privacy myopia'.[1360] The latter concept has to be contrasted with the 'nothing to hide' argument.[1361] This is because in the 'nothing to hide' argument the data subject appears to be aware of privacy of his or her personal information. Yet he or she compromises such value in the course of balancing it with other important values, more particularly security issues. However in some cases the 'nothing to hide' argument may itself be part of the 'privacy myopia'. This happens when a person who is in the first place suffering from the influence of 'privacy myopia' is misled to reveal his or personal information on the justification of 'nothing to hide'. In the African context, for example, this can well be illustrated by the compulsory registration of SIM card, which quite often proceeded partly on the basis of fight against crimes while no evidence merited those claims. In support of this view, Branttie posits:-

> 'First of all, the NCA and the Ministry of Communication(of Ghana) may not have had the hindsight of any empirical evidence supporting how registration of SIM cards has curtailed crime in any of the jurisdictions where this exercise has been implemented. Instead, there have been concerns about whether the exercise was really necessary at all, and its direct effect, or indirect effect for that matter, has not been evident as regards to a lowering crime rate, prank calling or money laundering.'[1362]

Extending the concept of 'privacy myopia' in the African context while explaining the value attached on privacy by individuals in Uganda, Bakibiknga argues that Ugandans largely suffer from 'privacy myopia'.[1363] This is also the case with other African countries such as Nigeria as already explained by Kusamotu.[1364] Yet, lack of awareness of privacy risks should not be regarded as a natural phenomenon. There are complex arrays of factors which offer explanation to this condition. The latter include the low level of computerisation or penetration of technology in Africa which result in the corresponding low level of data processing and awareness about its implications for privacy.[1365] This penetration level has resulted in 'digital divide' between urban

[1360] Froomkin, pp.1502-1506, note 6, supra.
[1361] Solove, D.J., "I've Got Nothing to Hide" and Other Misunderstandings of Privacy', San Diego Law Review, 2007, Vol.44, No.4, pp.745-772.
[1362] Branttie, p.1, note 1298, supra.
[1363] Bakibinga, notes 61 and 176, supra.
[1364] Kusamotu, notes 166 and 178, supra.
[1365] Ibid.

and rural Africa. Another factor affecting awareness is high level of illiteracy in Africa.[1366] With this general illiteracy level, individuals' ability to understanding threats posed upon their privacy becomes severely limited. However this does not suggest that literate individuals are well placed to understand privacy risks of their personal information. A recent survey conducted across Africa, '*Awareness Survey on Freedom of Information and Data Protection Legislation and Open Government Data Initiatives*'[1367] from 27 to 30 September 2011, provides solid evidence that lack of awareness of privacy risks affects a large number of literate individuals working in private sectors, governments, academic and researcher institutions. This survey asked the following question in the context of data protection legislation: does your country have a data protection law? The results were as follows: 36% said yes, 19% said no and 45% said do not know.[1368] Yet, when mapped against the actual existence of data privacy legislation in each country it was found that many of the responses were not correct. Sometimes participants replied yes while such data privacy legislation did not exist or replied no while such legislation exists or replied do not know while a data privacy legislation exists or does not exist.[1369] Although this survey was not meant to be rigorously scientific, it gives a snapshot of how much and what people know about data privacy in their countries.[1370] Admittedly, while being aware of privacy risks does not necessarily mean that one must know the existence of legislation yet the vice-versa may be true. This survey reflects Bygraves' views in the following paragraph:-

> 'Data protection laws are recent additions in the legal landscape; the first such laws were not enacted until the early 1970s. Though a large number of legal and quasi-legal instruments on data protection are now to be found, they still tend to be an unknown or poorly known quantity for many people, lawyers included.'[1371]

Apart from the above factors affecting awareness, it is difficult to disagree entirely that African culture impacts on an individual's awareness and consciousness for privacy, particularly in rural areas where collectivist style of life is still discernible. As pointed out by some commentators,

---

[1366] See e.g., UNESCO, Institute for Statistics. 'Adult and Youth Literacy', Facts Sheet, September 2011, http://www.uis.unesco.org/FactSheets/Documents/FS16-2011-Literacy-EN.pdf last visited 2/03/2012.

[1367] Taylor, K., 'Awareness Survey on Freedom of Information and Data Protection Legislation and Open Government Data Initiatives', The Internet Governance Forum, Nairobi, Kenya, 27th -30th September 2011, pp.1-19,
http://epsiplatform.eu/sites/default/files/IGF6_W123_PSISurveyreport_21October2011.pdf,
last visited 2/03/2012.

[1368] Ibid, p.3.

[1369] Ibid, pp.5-15.

[1370] Ibid, p.5.

[1371] Bygrave, p. 2, note 24, supra.

through group association in African cultures an individual's interests are subordinate to group's. Accordingly, there is sharing of even sensitive personal information with others without knowing the likely resulting privacy risks. Yet, while collectivist culture operates as a negative determinant, there has been rare discussion let alone mention of culture in the legislative processes and the data privacy laws' *trauvaux préparatoires* leading to data protection legislation in Africa.[1372] This may be partly due to two main factors: over dominance of economic justifications for adopting such legislation as state-sponsored agenda as well as its attendant propaganda and lack or inadequate public consultation during the legislative processes of data privacy laws (see below).

- **Resistance to Transparency**

Some governments resist taking interest in privacy issues because they do not want to become more and more transparent and accountable to their people. This resistance can be demonstrated generally by the rejection of the Bill of Rights in the independence constitutions or restricting its application; rejection of access of information legislation or restriction of their application; and specifically being indifferent in initiating legislative process for data protection legislation which in some ways puts governments under certain obligations in processing personal information. This in turn limits the ability of governments to conduct unregulated surveillance over its people.

- **Lack or inadequate Legislative Consultation**

Historically the drafting and enactments of data protection laws around the world, particularly in Europe have frequently been lengthy processes fraught with controversy.[1373] Yet, in some places like Sweden, preparation and enactment of data protection legislation occurred relatively quickly and smoothly.[1374] However this does not suggest that data privacy legislation in Sweden was adopted without public consultation or in just few days. In Africa, with exception of only few countries (e.g. South Africa), the enactments of data privacy legislation had not engaged public consultation or such consultation had been inadequate. Ordinarily, public consultations in the legislative process generate debates about the need or otherwise of data privacy laws, their contents, enforcement, etc and in the course of that stimulates interests and awareness in these laws to the public. Concomitantly, they facilitate implementation of data privacy laws once enacted.

[1372] See chapters 5, 6 and 7 of this thesis.
[1373] Bygrave, p.4, note 24, supra.
[1374] Ibid, p.5.

- **Cost**

The cost of adopting and implementing comprehensive data protection legislation is also among critical issues to developing countries. Such cost is borne with respect to carrying out training, awareness programmes, seminars, carrying out investigations, dispute resolution, etc. As most African governments' annual budgets depend to over 30% of budget support from donors,[1375] it is practically difficult to finance the adoption and implementation of data privacy legislation (see 4.4.2.2(b)).

4.3.2 Concepts and Theories of Privacy in Africa

So far there is neither concept nor theory that uniquely deals with privacy in an African cultural context. The specific call for conceptualization of privacy in an African context appears only in the works of Bakibinga. As pointed out, Bakibinga holds that an individual in Africa can have privacy and still be part of the community.[1376] Building upon this premise she makes a definitive call specifically for her country (Uganda) that privacy has to be defined in a way that is acceptable to the Ugandan society given the emphasis on communalism versus individual rights.[1377] She also contends that privacy should not remain an abstract and one way to start would be to commission studies to obtain perceptions of privacy within the Ugandan society.[1378] It is really difficult to comprehend how a privacy concept can at one and the same time function to serve individual and group interests. A similar paradox in the Western privacy discourse can well be illustrated by Westin's definition of privacy which states that privacy is a claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[1379] Interestingly reference to 'group' in the Westin's definition of privacy is not repeated in other Western theories of privacy. Instead, an individual is the primary reference point in such theories.

The only theory of privacy that has started to gain prominence in Africa, albeit not in the African cultural context as such, is that of a renowned Professor Johann Neethling. Neethling's theory of privacy states:-

---

[1375] Knoll, M., 'Budget Support: A Reformed Approach or Old Wine in New Skins?' UNCTAD Discussion Papers, No. 190, October 2008, pp. 1-13, at p.1,
http://www.unctad.org/en/docs/osgdp20085_en.pdf last visited 14/03/2012.
[1376] EPIC, note 60, supra.
[1377] Bakibinga, note 61, supra.
[1378] Ibid.
[1379] Westin, note 410, supra.

> 'Privacy is an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy.'[1380]

The above definition implies that privacy is an absence of acquaintance with a person or his personal affairs in his state of seclusion.[1381] Accordingly, privacy can only be infringed by the unauthorized acquaintance by an outsider with a person or his personal affairs, which acquaintance can occur in two ways only: first, by intrusion in the private sphere(that is, where an outsider himself becomes acquainted with a person o has personal affairs); and, secondly, by disclosure or revelation of private facts(that is, where a third party acquaints outsiders with a person o his personal affairs which, although known to that party, remains private).[1382] As privacy is closely associated to other personality interests, Neethling has spent a considerable space in his literature, while criticizing his rivals and some South African court's decisions, to distinguish it from such other interests: physical-psychological integrity (including sensory feelings); dignity; identity; autonomy; self-realization and patrimonial interests.[1383]

Although Neethling's theory of privacy appears to be postulated in 1976,[1384] the same is not novel. Neethling seems to have relied on a similar theory as propounded by Hyman Gross in 1967.[1385] The context in which Gross' conceptualization of privacy sprang was the U.S Supreme Court's decision in *Griswold v Connecticut*.[1386] In this way it can be argued that Neethling's theory of privacy follows the same pattern of the Western individualism. Also important, such theory can be classified as falling under the control theory of privacy concept. Despite that, Neethling's theory of privacy has received wider recognition in literature in South Africa and in other countries within Africa. Roos, Anspach and Nwauche serve as commentators in Africa who are fond of Neethling's

---

[1380] Neethling, J *et al*., Neethling's Law of Personality, Butterworth, Durban, 1996, p.36; Neethling, J *et al*, (Neethling's Law of Personality), p.32, note 186, supra; Neethling, J., 'The Concept of Privacy in South African Law', The South African Law Journal, 2005, Vol.122, No.1, pp.18-28, at p.19; Neethling, J *et al* (Law of Delict), p.347, note 186, supra.

[1381] Neethling (The Concept of Privacy in South Africa Law), p.21, note 1380, supra.

[1382] Ibid.

[1383] Ibid, pp.22-27; see also, Neethling, *et al* (Neethling's Law of Personality), note 186, supra; Neethling, J *et al*(Law of Delict), pp.346-354, note 186, supra; Currie, I., 'The Concept of Privacy in the South African Constitution: Reprise', Journal of South African Law, 2008, Vol.2008, No. 3, pp.549-557.

[1384] Neethling, J., *'Die Reg op Privaatheid'*, LL.D Thesis, UNISA, 1976.

[1385] Gross, H., 'The Concept of Privacy', New York University Law Review, 1967, Vol.42, No.1, pp.34-54.

[1386] 381 U.S. 479 [1965].

theory.[1387] Similarly, Neethling's theory of privacy has received the approval of the South African Supreme Court of Appeal in *National Media Ltd v Jooste*.[1388]

Putting Neethling aside, other commentators in Africa have avoided debates about the concept of privacy. Instead, and for certain purposes, they tend to apply one or more definitions of privacy from the Western discourse. This means that the African understanding of privacy is not dissimilar to definitions postulated by Western scholars. The similarity alluded to here is partly due to the fact that privacy is an imported concept in Africa from the Western culture.

4.4 Policy and Regulatory Frameworks for Privacy and Data Protection

Policy and legal regulation of privacy and personal data protection in Africa can be analyzed in three clusters: regional, sub-regional and national levels. At the regional level various instruments have been developed under the auspices of the African Union (AU). Under sub-regional level there are initiatives by Economic Community of West African States (ECOWAS), East African Community (EAC), and Southern African Development Community (SADC). Fewer initiatives are known to have taken place in the Common Market for Eastern and Southern Africa (COMESA) and Economic Community of Central African States (ECCAS), and Arab Maghreb Union (UMA).

4.4.1 Regional Frameworks

The policy and regulatory frameworks for privacy and data protection at the regional level are those developed under the initiative and auspices of the African Union (AU). Three instruments are considered at the exclusion of any other initiatives because they are directly affecting the issues addressed in this thesis. For precision, the three instruments are: the African Charter on Human and Peoples' Rights 1981 (ACHR or the Banjul Charter); the African Charter on the Rights and Welfare of the Child 1990 (ACRWC or the Children's Charter); and the Draft African Union Convention on establishment of a credible legal framework for cyber security in Africa 2011 (Convention on Cyber Security).

[1387] Roos(LL.D Thesis), pp.554-560, note 2, supra; Anspach, p.66, note 1235, supra; Nwauche, p.78, note 179, supra.
[1388] [1996] 3 SA 262(A) 271.

4.4.1.1 African Charter on Human and Peoples' Rights 1981

The African Charter on Human and Peoples' Rights 1981 is the main human rights treaty for the African Union (AU).[1389] The latter (formerly known as the Organization of African Unity until 2009) is a union of 54 members except Morocco.[1390] The objectives of the African Union are to promote unity and solidarity among the member states; to foster socio-economic integration of the continent; to promote and defend African common positions on issues of interests to the continent and its peoples; to achieve peace and security; to eradicate all forms of colonialism from Africa and to promote international cooperation having due regard to Charter of the United Nations and the Universal Declaration of Human Rights.[1391] Perhaps it was this latter objective which partly necessitated the adoption of the ACHR in 1981.

In terms of privacy, the African Charter on Human and Peoples' Rights does not provide expressly for its protection. This omission has erroneously led many commentators to conclude that Africans do not value privacy.[1392] Yet, recently some commentators have advanced argument that despite such an omission, privacy can still be read in other provisions protection personality rights, particularly the right on dignity.[1393]

4.4.1.2 African Charter on the Rights and Welfare of the Child 1990

The African Charter on the Rights and Welfare of the Child 1990[1394] (ACRWC) is the only AU's instrument which expressly guarantees the right to privacy. Article 10 of this Charter states: 'no child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.'

[1389] OAU, African Charter on Human and Peoples' Rights, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), 27 June 1981, entered into force 21st October 1986.
[1390] Currently the African Union has the following members: Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Democratic Republic of Congo, Republic of Congo, Côte d'Ivoire(Ivory Coast), Djibouti, Egypt, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guinea-Bissau, Guinea, Kenya, Lesotho, Liberia, Libya, Malawi, Mali, Mauritania, Mauritius, Mozambique, Namibia, Niger, Nigeria, Rwanda, Sahrawi Arab Democratic Republic, São Tomé and Príncipe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Swaziland, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe. Madagascar has been suspended since 2009.
[1391] OAU Charter 1963, Article II(1).
[1392] See e.g., Gutwirth, note 46, supra; Bygrave, note 559, supra; Bakibinga, p.9, note 38, supra; Burchell, (footnote 3), note 77, supra.
[1393] Enyew, p.15, note 1336, supra.
[1394] OAU, note 136, supra.

As argued before, the adoption of the ACRWC collapses any argument that the omission of a provision for protection of privacy in the ACHPR is sufficient evidence to support the claim that Africans do not value privacy. However one point must be clearly made out, the main influence on the adoption of the ACRWC is the United Nations Convention on the Rights of the Child 1989.[1395] The right to privacy is one of the provisions of the United Nations Convention. Yet, it is still not clear why the African Charter on Human and Peoples' Rights omits a clause on protection of privacy despite the fact that it makes reference in its preamble to the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights. Interestingly, these two instruments contain clear provisions on protection of the right to privacy. As already submitted, the provisions on the rights to privacy in the UDHR and ICCPR apply directly in some African countries whose treaty practice is monism. Moreover, in dualist African states these provisions have permeated into national constitutions as well.

4.4.1.3 African Union Convention on Cyber Security 2011

The African Union Convention on Cyber Security 2011(i.e. Cyber Convention)[1396] is still a draft convention in legislative process. Significant changes are not expected in the final law because of the context in which the Convention arose. This context is considered below. Partly because of this and also the fact that the draft Convention has substantially replicated the ECOWAS sub-regional data privacy law, it is worth important to make comments on it, more particularly on provisions relating to regulation of data privacy.

The development of the draft Cyber Convention traces back into the Addis Ababa Declaration by the Heads of State and Government of the African Union on 2 February 2010.[1397] In this Declaration, it was alluded to that ICTs are powerful catalysts for the development and integration process in Africa. It was realized that ICTs need to be regulated in that regard. Because of this, the establishment of a legal and regulatory framework that is harmonized and

---

[1395] United Nations Convention on the Rights of the Child 1989; adopted on 20th November 1989 and entered into force on 2nd September 1990.

[1396] AU, Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, Version 01/01.2011, http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf last visited 4/03/2012.

[1397] AU Addis Ababa Declaration on Information and Communication Technologies in Africa: Challenges and Prospects for Development, Assembly/AU/Decl.1(XIV), Adopted by the Fourteenth Ordinary Session of the Assembly in Addis Ababa, Ethiopia on 2nd February 2010.

attractive for investments, shared telecommunications and ICT infrastructure as well as the convergence of networks, services and administration became necessary. In the context of the Addis Ababa Declaration, the draft Cyber Convention became developed. This Convention is currently under consideration by the AU organs.

Structurally, the Draft Cyber Convention has two main parts: the introductory matters which give the general context in which the Convention is being drafted and the Convention itself. The latter is divided into five sections. The first section comprises the preamble with fourteen recitals. The rest four sections are titled as 'parts'. Part I comprising Arts I (1)-I (39) deals with Electronic Commerce. Part II starting from Art II (1)-II (50) deals with Protection of Personal Data. Undoubtedly this is the longest part in the Convention. Part III covering Arts III (1)-III (41) is devoted on matters of Cyber Crimes. Part IV which is the final, covers Arts IV (1)-IV (7) on Common and Final Provisions.

Briefly, the context in which the African Union has proposed the Cyber Convention largely rests on the development of information and communications technologies (ICTs) in the continent and the risks and challenges posed by them. In particular, African countries are concerned by the globalization of risks, crimes and threats to cyber security. This concern is reflected in the broad objective and goal of the draft of Cyber Convention in paragraph 3 of its introductory section which states:-

> 'The objective of the Convention on Cyber Security is to contribute to the preservation of the institutional, human, financial, technological and informational assets and resources put in place by institutions to achieve their objectives. The Convention embodies the treatment of cyber crime and cyber security in its strict sense, but is not confined solely to these elements. It also embraces important elements of electronic commerce and the protection of personal data.'

Also important to note, the proposed Cyber Convention has been prompted by the need to achieve harmonisation of cyber laws across Africa. The harmonisation agenda manifests from the tendency by some African states to increasingly enact legislation on cyber security and ICTs in general. This tendency is also growing at sub-regional level, particularly in ECOWAS where

cyber law treaties have been adopted to regulate various issues. The overall result of these uncoordinated initiatives is divergences in legal standards and distortion of internal markets.

As pointed out, Part II of the draft Cyber Convention contains data protection regulations. This is the only part directly relating to this thesis. A close observation of Part II of the Cyber Convention leaves no doubt that the same largely incorporates the ECOWAS' Data Protection Act with few slight modifications.[1398] Yet, both the ECOWAS' Data Protection Act and Part II of the Cyber Convention are modelled on the European Directive 95/46/EC on protection of individual personal data. Because of this, it can be submitted that Part II of the AU's Cyber Convention contains both the basic principles of data processing as well as the requirement of supervisory authorities to implement data protection legislation at national level. The main features of Part II of the Cyber Convention are considered below.

Article II (1) of the Cyber Convention defines various concepts used in the text. Most of these definitions are the same as those provided in Article 2 of Directive 95/46/EC. However it is interesting to note the use of new terminologies with the same meanings as in the Directive. For example, 'data controller' in the Directive has the corresponding meaning to 'data processing official' in the Cyber Convention; 'data subject' is equivalent to 'person concerned' in the Cyber Convention. The case is also the same with 'processor' in the Directive which corresponds to 'sub-contractor' in the Convention. Interesting also to observe, is the use of the term 'direct prospecting' which means any solicitation carried out through message dispatch, regardless of the message base or nature, especially messages of commercial, political or charitable nature, designed to promote, directly or indirectly, goods and services or the image of a person selling the goods or providing the services. This definition is absent in the Directive 95/46/EC but the same appears narrowly as 'direct marketing' in Directive 2002/58/EC (Directive on privacy and electronic communications)[1399] as amended by Directive 2009/136/EC.[1400]

[1398] ECOWAS, Supplementary Act A/SA.1/01/10 on Personal data Protection within ECOWAS adopted in Abuja on 16th February 2010.

[1399] Directive 2002/58/EC on the European parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J.L 201, pp.0037-0047, dated 31/07/2002. as amended by Directive 2009/136/EC of the European parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, O.J.L 337, pp.11-36 dated 18/12/2009.

[1400] Directive 2009/136/EC of the European parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the

The objectives of the Cyber Convention with regard to protection of personal data are stated in Art II (2). This provision provides that each member of the African Union 'shall put in place a legal framework with a view to establishing a mechanism to combat breaches of private life likely to arise from the gathering, processing, transmission, storage and use of personal data.' In broad terms Art II(2) proceeds to state that such mechanism must ensure that any processing of personal data, respects the freedom and fundamental rights of physical persons while at the same time recognising the prerogatives of the state, the rights of local communities and the interest of enterprises. It is imperative to note that this objective is slightly different from those in the Directive. First, it has been formulated in terms of prevention of breaches of private life while that in the Directive relates to protection of the right to privacy. Second, the Cyber Contention seems not to put emphasis on free flow of personal information across the African Union as it is the case with the Directive in the European Union. Perhaps this is partly because so far there have been no serious impediments to this flow of information. Yet when Art II(1) is read in conjunction with recitals 7 and 8 of the Convention, the guarantee of the free circulation of information stems out clearly as one of the objective of the Convention. Also, the reference to protection of privacy appears to qualify the breaches of private life. However recital 7 is problematic in its formulation. It restricts the protection of privacy to citizens suggesting that non-citizens (i.e. foreigners) cannot be afforded protection. Since this is just a draft, it remains to be seen if adopted, how this provision will be implemented as currently some AU member states have already adopted data privacy legislation without this restriction while others have had this restriction already in their laws. Nigeria, for example, maintains this restriction and has been assessed by commentators in combination with other shortcomings as not providing adequate level of protection of personal data.[1401] Although attraction for investments is not clearly stated in the Cyber Convention, the Addis Ababa Declaration clearly points out that investment is one of the reasons for adopting such legal and regulatory framework on cyber-security issues.

The scope for the application of the Cyber Convention is stipulated in Art II-3. Accordingly, Cyber Convention applies to private and public sectors. In both cases the Convention extends its application to processing of personal information of natural person and legal entities. Moreover, the Convention targets both automated and non-automated (i.e. manual) processing of personal data. The territorial application of the national data privacy is restricted by the Cyber Convention

electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, O.J.L 337, pp.11-36 dated 18/12/2009.

[1401] Kusamotu, note 165, supra.

to processing of data taking place in the territory of a member state. This to say is the choice of law rule in the Cyber Convention. It is based on the territoriality principle akin to Art 4 of the Directive 95/46/EC but less complex as the latter. To be precise, the territoriality principle in the Cyber Convention is similar to Art 4(1) (a) of the Directive which places emphasis on the law of a member state to apply when processing activities have taken place. Yet, it falls short of Art 4 because it does not cover those situations in 4(1) (b) and (c) where national law applies by virtue of public international law and where there is a use of 'equipment' in the territory of a member state respectively. It is imperative to note that these latter situations apply in relation to third countries. Also contrary to the Directive which excludes activities falling outside the scope of the Community law (e.g., processing operations concerning public security, defence, state security and criminal law), the Cyber Convention subjects these processing operations under its general scope. Yet the Convention gives the member states a leverage to make exceptions under specific provisions of national legislation. Since the scope of these leverages is not clear, in practice a state may exclude entirely the application of the Convention on such types of data processing.

The Cyber Convention intends not to apply in two areas: where processing takes place within the exclusive context of personal or domestic activity and where temporary copies produced within the context of technical activities for transmission and access to a digital network for the sole purpose of offering other beneficiaries of the service the best possible access to the information so transmitted. While the first exception in the Cyber Convention is similarly found in Directive 95/46/EC, it is further qualified: that is, such data processing is not meant to be carried out for systematic communication to third parties or for further dissemination. Practically, this additional qualification does not serve any value as any processing concealed to be undertaken under the cover of personal or domestic activities and subsequently discovered to be inconsistent with such purposes and limits will automatically be taken to fall short of this exception. As to the second exception, an equivalent provision is lacking in the Directive 95/46/EC. Perhaps this can be related to the proviso in Art 4(1)(c) of the Directive, which seems to exclude its application in case an 'equipment' is used solely for purposes of transit of personal data through the territory of the community. Yet, significant differences are still noticeable. In the Cyber Convention, there are temporary copies created during transmission of personal data. These can be accessed by beneficiaries making potentials for disclosure of individual's personal data. Accordingly, this second exception in the application of Cyber Convention undermines its objective.

The Cyber Convention contains seven basic principles of data processing reflecting the ones provided in Directive 95/46/EC. However there are significant differences in ambit and scope in certain cases.

The first principle is the principle of consent and legitimacy of personal data processing.[1402] This principle states that processing of personal data shall be deemed to be legitimate where the person concerned has given his/her consent. However, there are four exceptions to this general requirement: where processing is necessary for compliance with a legal obligation in which the processing official is subject; processing is necessary for executing a mission of public interest or deriving from the exercise of public authority vested in the processing official or third party to whom the data have been communicated; processing is necessary for executing a contract to which the concerned person is party or pre-contractual measures undertaken at his/her request; and finally where processing is necessary to safeguard the interest or fundamental rights and freedoms of the person concerned. The consent and legitimacy of processing of personal data principle under the Cyber Convention somewhat corresponds to Art 7 of Directive 95/46/EC, particularly paragraphs (a) to (e). Yet, three significant differences can be noted. The Cyber Convention considers 'consent' as the single primary criterion for legitimising data processing and only regards the four exceptions as subordinate to 'consent'. This is not the case under the European Directive where 'consent' is put at the same level as other legitimising criteria. Also, criterion (f) in the Directive on processing personal data for the purposes of the legitimate interest pursued by the controller or 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 required under the Directive, is missing in the Cyber Convention. This makes the Convention more restrictive than the Directive. Moreover, the Directive is more specific and protective in using the expression 'vital interests of the data subject' in one of the legitimising criteria as opposed to the expression 'safeguard the interest or fundamental rights and freedoms' used in the Cyber Convention. In the former case, an element of balancing various interests emerge and is highly likely to be resolved in the advantage of the data subject than in the Cyber Convention.

The second is the licitness and honest of personal data processing principle.[1403] This principle states that the gathering, registration, processing, storage and transmission of personal data shall

[1402] AU, Cyber Convention, Art II-28.
[1403] Ibid, Art II-29.

be undertaken licitly, with honesty and non-fraudulent. It is equivalent to the principle of fairness and lawfulness of processing under Art 6(1) (a) of the Directive.

The third principle is formulated as the principle of objective, relevance and conservation of processed personal data.[1404] It requires that data gathering to be undertaken for a set objective that is explicit and legitimate. Further processing in a manner incompatible with the original objectives is prohibited. This principle also requires that data gathered must be adequate, relevant and non-excessive in relation to the ultimate objective for which they have been gathered and subsequently processed. With exceptions of processing undertaken for historical, statistical or research purposes, data must only be conserved for the duration not exceeding the period required to achieve the ultimate objective for which they were gathered. This principle corresponds to the principles of purpose specification, adequacy and relevancy in Arts 6(1) (b), (c) and (e) of the Directive.

The fourth principle is the accuracy of personal data.[1405] Like its corresponding principle in Art 6(1) (d) of the Directive, it requires that personal data collected must be accurate and kept up to date. Every reasonable step must be taken to ensure that data which are incorrect and incomplete in relation to the purpose for which they were collected and further processed are deleted or corrected.

The fifth principle is the transparency of personal data.[1406] This principle requires data processing officials to provide information on personal data. Yet, it does not specify which information is to be given, to whom and in which manner. However the details of such information are provided in Art II-43. The transparency principle in the Convention partly reflects Art 10 of the Directive. However the Directive is broader in that under Art 11 another set of information is required where personal data is not collected from the data subject directly.

The sixth principle is confidentiality and security of personal data processing.[1407] This principle is otherwise known as the principle of information security. It places obligation on the part of the processing official to process data confidentially and protect it. Much emphasis on this principle is placed when processing involves transmission of the data in a network. Further, it requires that

[1404] Ibid, Art II-30.
[1405] Ibid, At II-31.
[1406] Ibid, Art II-32.
[1407] Ibid, Art II- 33 and 34.

when processing is undertaken on behalf of a processing official, the latter must choose a sub-contractor with adequate guarantees. Both are required to ensure compliance with security measures defined in the Cyber Convention. Yet, such measures are no where defined in Part II of the Convention or in any other parts. In contrast, Arts 16 and 17 of the Directive are more detailed and clearer than the Cyber Convention. For example, Art 16 provides clearly that the data processor or a person working under him, must process personal data only according to instructions from the controller, unless he is required to do otherwise by law. Art 17 stipulates a list of threats that must be prevented and how. As the Cyber Convention, Art 17 requires that whenever a data controller chooses a processor the latter must guarantee sufficient level of security. However, contrary to the Convention which is silent on the modality of the relationship between the data controller and processor, the Directive requires that the processor to be bound by a contract or legal act stipulating that the latter shall only process data on instructions from the employer. The obligations defined under the law in the member state shall also be incumbent on the processor. Furthermore, for purposes of proof, the contract or legal act is required to be kept in writing. Compared, the Directive seems to provide stronger safeguards in terms of security than the Convention.

The seventh principle comprises a set of principles governing the processing of certain categories of personal data. The first category of such principles is the sensitivity.[1408] The latter prohibits processing of personal data based on racial, ethnic and regional considerations, parentage relationship, political views, religious or philosophical persuasion, trade union membership, sex life and genetic information or, more generally, and data on the state of health of the person concerned. This principle is somewhat broader than Art 8 (1) of the Directive in terms of the list of prohibited processing. However, the Convention provides a list of ten exceptions in which the sensitivity principle does not apply. These include where processing involves data manifestly published by the person concerned; the person concerned has given his/her written consent, by whatever means; processing of personal data is required to safeguard vital interest of the person concerned; processing of personal data involves genetic data, in particular required for investigation purposes, and exercise or defense of the right to justice; a judicial procedure or criminal investigation has been opened; processing of personal data is required in the public interest; processing is required in order to execute a contract to which the person is party or pre-contractual measures undertaken at the request of the person concerned; processing is necessary to obtain compliance with a legal order or regulatory obligation to which the processing official

[1408] Ibid, Art II-35 and 36.

is subject; processing is required to execute a mission of public interest or a mission undertaken by a public authority to the processing official or assigned by a public authority to a processing official or to a third party; or processing is undertaken within the framework of the legitimate activities of a foundation, association or any other non-profit making body or for political, philosophical, religious, self-help or trade union purposes. In this latter provision, the processing must only concern members of the said body or persons in regular contact within the framework of their activities and not disclosed to a third party without the consent of the person concerned.

The sensitivity principle under the Convention is similar to Art 8 of the Directive with only few modifications. For example, while the former makes reference to 'written consent' as one of the exceptions for processing sensitive personal data, the latter refers to 'explicit consent'. Also, the requirement for processing in the context of 'mission of public interest' in the Cyber Convention is missing in the Directive. Yet, the Directive leaves room for member states to introduce additional exceptions to the principle of sensitivity in their national laws while this is not the case in the Convention. This implies that the EU member states may have wider exceptions than AU member countries.

The other principle for processing certain categories of personal data includes processing for journalistic purposes or research or artistic or literary expression.[1409] Processing of personal data under these categories is only subject to the code of conduct of the respective professions. With the exception of research, this requirement is similar to Art 9 of the Directive.

Furthermore, Art II -38 provides that the provisions of the Cyber Convention shall not impede the application of laws relating to the print media or the audio-visual sector and the provisions of the penal code which prescribe the conditions for the exercise of the right of response, and prevent, restrict, compensate for and, where necessary, repress breaches of private life and the reputation of physical persons. This provision is lacking in the Directive. The Cyber Convention also contains rules prohibiting direct prospection unless the person concerned has given prior consent which are quite broader.[1410] While similar rules are not present in the Directive, the same are provided in the Electronic Communication Directive as direct marketing.

As regard automated processing, the Cyber Convention provides narrower principles than the Directive. Art II-40 of the Convention prohibits automated processing in two circumstances:

[1409] Ibid, Art II-37.
[1410] Ibid, Art II- 39.

where a legal ruling involving an appraisal of the comportment of a person and where a decision produces legal effect on a person. While the Convention seems to contain absolute prohibition on automatic processing, the Directive has provided exceptions to the general principle in Art 15(2). Moreover, the Directive prohibits not only automated processing that produces legal effects but also that which significantly affects the data subject.[1411]

The other principle for processing special categories of personal data is about interconnection of personal data files or data matching.[1412] The latter is permitted subject to the authorisation of the protection authority as per Art II-8 of the Cyber Convention. Moreover, interconnection is limited to help attain the legal or statutory objectives that present legitimate interest for data treatment officials. Interconnection is required to avoid discrimination or erosion of the rights, freedoms and guarantees in respect of the persons concerned. Yet, it is not supposed to be loaded with security measures. The underlying principle in any case of interconnection is the relevance of the data required to be interconnected.

Apart from the above basic principles of data processing, the Convention contains a set of rights of data subject and obligations on the part of the processing official. The set of rights comprises the following: the right to information; right to access; right to opposition and right of correction or suppression.[1413] These rights are similar to those in Arts 10, 11, 12 and 14 of the Directive. Yet there are some significant differences in some aspects. For example, under the African Union's Cyber Convention the data subject has the right to request to feature no longer in the file.[1414] While this provision is not available in the Directive, it is akin to the 'right to be forgotten' in the proposed EU General Data Protection Regulation 2012.[1415] Also, the provision on the right of access in the Convention is too limited to confirmation of certain information on personal data processed and the purpose for such collection as well as their communication to the data subject. This is contrary to the corresponding right of access in Directive 95/46/EC which goes far to understand knowledge of the logic involved in any automatic processing of data concerning the data subject in the case of automated decisions. Another important dissimilarity between the Convention and the Directive is that the latter puts as a right of access to the notifications of any rectification, erasure or blocking made by the data controllers to third parties to whom the data have been disclosed.

[1411] Directive 95/46/EC, Art 15(1).
[1412] AU, Cyber Convention, Art II-42.
[1413] Ibid, Art II-43, 44, 45 and 46 respectively.
[1414] Ibid, Art II-43(5).
[1415] EU General Data Protection Regulation, Art 17.

As regards obligations, the Cyber Convention places the obligations of confidentiality; security; conservation; and sustainability on the part of the processing official.[1416] These corresponding obligations scatter in the Directive with varying scope and ambit.

Like Directive 95/46/EC, the Cyber Convention contains rules on transborder data movement although it adopts 'sufficient level' standard as opposed to 'adequacy level' standard in the Directive. Art II-41 states that the data processing official shall not transfer personal data to a non-Member state of the African Union unless such a state offers sufficient level of protection of the private life, freedoms and fundamental rights of persons whose data are being or likely to be processed. This provision requires further that before any personal data is transferred to a third country; the data processing official shall give prior notice of such transfer to the protection authority. However, contrary to the Directive, the Cyber Convention does not provide criteria for assessing the level of adequacy of data protection nor does it expressly indicate who is to undertake such assessment. Despite this omission, the Cyber Convention places obligation on the part of national protection authority to authorise cross-border transfer of personal data.[1417] This may suggest that while at the African Union level there is no anybody charged with the duty of assessing the level of adequacy of data protection in the third countries; at the national level such mandate is performed by the national protection authority on a case to case basis. Yet, there is no requirement of notifying national protection authorities in other member states of any finding as to the level of protection of personal data in the third country. Also important to note, the Cyber Convention does not lay down any rules of exception that may still permit transfer of personal data to third countries where the adequacy level is not met. Undoubtedly, the rules of transborder of personal data from the African Union to third countries are very limited and are not compatible to the objective of free movement of personal data and harmonisation.

Institutionally, the Cyber Convention obliges every member of the African Union to establish an authority with responsibility to protect personal data.[1418] This authority is required to ensure that processing of personal data in their respective countries is conducted in accordance with the Cyber Convention.[1419] One way to ensure this compliance is to require a declaration before a protection authority of any personal data processing activity.[1420] As to its nature, the protection

[1416] AU, Cyber Convention, Art II-47, 48, 49 and 50 respectively.
[1417] Ibid, Art II-23(11).
[1418] Ibid, Art II-14.
[1419] Ibid.
[1420] Ibid, Art II-6.

authority is required to be an independent administrative authority.[1421] The independence of this authority is discernible in three areas. First, members of the protection authority should not be appointed from the governments (i.e. the executive branch).[1422] Instead, such members shall comprise parliamentarians, deputies, senators, senior judges of the tribunal, Council of State, Civil and Criminal Appeal Court, personalities qualified as a result of their knowledge of computer science, as well as professional networks or sectors;[1423] second, the protection authority is required to be afforded budgetary subvention for accomplishment of its missions;[1424] and finally members of the protection authority are required to enjoy full immunity for the views they express in the exercise or on the occasion of the exercise of their functions.[1425] Moreover members of the protection authority are not required to receive instructions from any authority in the exercise of their functions.[1426] It is imperative to note that although the corresponding provision in the Directive refers to 'complete independence' as opposed to just 'independence' in the Cyber Convention, the two provisions have the same meaning.[1427] Other requirements which apply to the members of the protection authority include the duty of secrecy.[1428] The protection authority is similarly required to formulate rules of procedure governing deliberations, processing and presentation of cases.[1429]

In discharging its functions, the protection authority may impose sanctions, both administrative and pecuniary, on the defaulting data processing official.[1430] In particular, the authority may issue a warning to any data processing official that fails to comply with the responsibilities arising from this Convention or a formal demand for an end to any particular breaches within a timeframe set by the authority.[1431] Where the data processing official fails to comply with the formal demand addressed to him/her, the protection authority may impose the following sanctions after adversarial proceedings: provisional withdraw of licence; definitive withdraw of licence; or pecuniary fine.[1432] Moreover, in case of emergency, the protection authority may interrupt data processing; lock up some of the personal data processed; or prohibit temporarily or definitively

[1421] Ibid, Art II-14.
[1422] Ibid, Art II-19.
[1423] Ibid, Art II-16.
[1424] Ibid, Art II-21.
[1425] Ibid, Art II-20.
[1426] Ibid.
[1427] ECJ, notes 944 and 945, supra.
[1428] AU, Cyber Convention, Art II-18.
[1429] Ibid.
[1430] Ibid, Art II-23(8).
[1431] Ibid, Art II-24.
[1432] Ibid, Art II-25.

any processing at variance with the provisions of the Convention.[1433] The sanctions imposed and decisions taken by the protection authority are subject to appeal.[1434] However, in contrast to the Directive, the Convention does not say where appeals lie.

4.4.2 Sub-Regional Frameworks

4.4.2.1 Economic Community for West African States

ECOWAS is the Economic Community for West African States with fifteen members.[1435] It was established by the Treaty of Lagos on 28 May 1975 with the objective of promoting cooperation and economic integration in the West African region through harmonization of policies and laws.[1436] The Supplementary Act on the Harmonization of Policies and the Regulatory Framework for the Information and Communication Technology (ICT) Sector 2007[1437] is one of the greatest achievements towards those objectives. At least when compared to other sub-regions, ECOWAS is the most vibrant and dynamic organization in Africa.[1438] The other sub-regional groupings are considered in 4.4.2.2, 4.4.2.3, and 4.4.2.4.

In terms of data privacy protection, ECOWAS is the first and the only sub-regional grouping in Africa to develop a concrete framework of data privacy law: Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS.[1439] As pointed out, the ECOWAS Supplementary Act has been strongly influenced by the EU Directive.[1440] In turn the Supplementary Act has strongly influenced the African Union Cyber Convention. The latter has in fact replicated the former word-to-word with only few exceptions (see 4.4.1.3). Because of this, the analyses with regard to the Cyber Convention are wholly relevant for the ECOWAS Supplementary Act. This is despite the fact that the Convention may be adopted with significant changes or not.

[1433] Ibid, Art II-26.
[1434] Ibid, Art II-27.
[1435] Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo, see ECOWAS Website, http://www.ecowas.int/?lang=en last visited 10/03/2012.
[1436] ECOWAS Treaty 1975 as revised in 1991, http://www.worldtradelaw.net/fta/agreements/ecowasfta.pdf last visited 10/03/2012, Art 3.
[1437] Supplementary Act A/SA.1/01/07 on the Harmonization of Policies and the Regulatory Framework for the Information and Communication Technology (ICT) Sector 2007, adopted on the Thirty-First Session of the Authority of Heads of State and Government, Ouagadougou, 19th January 2007.
[1438] See e.g., Banjo, A., 'The ECOWAS Court and the Politics of Access to Justice in West Africa', CODESRIA Africa Development, 2007, Vol.32, No.1, pp.69-87, at p.70.
[1439] ECOWAS, note 1398, supra.
[1440] Greenleaf (Global Data Privacy Laws: 89 Countries, and Accelerating), p.7, note 38, supra.

Concomitantly, the discussion maintained in this part relates only to the main areas of differences between the Cyber Convention and the Supplementary Act.

Structurally, the ECOWAS Supplementary Act has a preamble with fourteen recitals and eight chapters. The latter comprise 49 articles in total. Chapter I titled 'General Provisions' has only one article, i.e. Art 1. This provision defines various concepts employed in the text. In total there are fifteen concepts defined under this provision similar to Art II-1 of the Cyber Convention. However there are two notable differences: the Cyber Convention omits to define 'Authority of Protection' which is available in the text and naming of some concepts. Data subject, data controller and data processor in the Supplementary Act correspond to personal concerned, data processing official and subcontractor yet with the same meaning.

Chapter II of the Supplementary Act titled 'Legal Framework for Personal Data Protection' is similar to Arts II-3, 4 and 5 of the Cyber Convention. The former has three provisions dealing with the aims and scope of the Act. It is imperative to note that the scope and aims of the two laws are the same except that whereas the Cyber Convention applies in the territory of a member state of the African Union the Supplementary Act applies to any processing of personal data carried out in a UEMOA[1441] or ECOWAS member state. Like the Cyber Convention the objectives of the Supplementary Act are protection of privacy and promotion of free movement of information. The same are clearly stated in the tenth and eleventh recitals of the preamble unlike in the text itself. In contrast to the Cyber Convention, the Supplementary Act takes as its objective the harmonization of data protection legislation already in existence prior to the Act.[1442] Moreover the legal vacuum generated by the use of the Internet is considered as a new invention of the Supplementary Act though there is little reference to the Internet in the content principles of the Act.

The basic principles of data processing in the Supplementary Act are contained in chapter V (Arts 23-37). This chapter corresponds to Art II-28 to Art II-42 of the Cyber Convention. The two sets of principles in these parts are the same. However there are two notable exceptions:

[1441] Union économique et monétaire Ouest Africaine (EUMOA) translating in English as the West African Economic and Monetary Union has the following member states: Benin, Burkina Faso, Cote d'Ivoire, Guinea-Bissau, Mali, Niger, Senegal, and Togo.

[1442] Recitals 10 and 11 of the ECOWAS Supplementary Act state: 'NOTING that, notwithstanding the existence of the national legislation relating to the protection of privacy of the citizens in their private and professional life and relating to the guarantee of the free movement of information, it becomes a matter of urgency to fill the legal vacuum generated by the use of internet which is a new instrument of communication; CONCIOUS of the necessity to fill this legal vacuum and establish a harmonized legal framework in the process of personal data.'

with regard to transfer of personal data to third countries, the Supplementary Act considers all other countries except members of ECOWAS as third countries. The latter includes the rest of the African countries as well as non-African countries. Yet, as currently only four ECOWAS states (Benin, Burkina Faso, Cape Verde and Senegal)[1443] have adopted data privacy legislation, the restriction of transborder data flow to countries without adequate level of protection in such laws may still impede movement of personal information within the ECOWAS itself. In contrast the Cyber Convention considers non-AU member countries as third countries (including African countries which are non-AU members such as Morocco and those suspended membership). However since ECOWAS countries are also members of the African Union, they are covered by the Cyber Convention. There are little chances for the Cyber Convention and Supplementary Act to conflict each other on this aspect simply because the two legal instruments are almost identical except for their geographical scope. However in any case of such conflict the former will likely prevail over the latter for being a regional law. Yet, the different ways of transposing these instruments in national laws leaves possibilities of problems of harmonization similar to those currently facing the European Union. Chapter VI of the Supplementary Act with four provisions (Arts 38-41) stipulate the rights of the individual whose personal data are the subject of processing. These are identical to Arts II-43, 44, 45 and 46 of the Cyber Convention. At the same time the Supplementary Act contains four provisions (Arts 42-45) on obligations of the data controller which are the same as Arts II-47, 48, 49 and 50 of the Cyber Convention.

Institutionally, the Supplementary Act and the Cyber Convention contain the same provisions. In the former case the governing provisions are Arts 14-22 of chapter IV while in the latter Arts II-14 to II-27. There are three differences. The first resides in the requirement of establishment of the protection authority. In contrast to the Cyber Convention, the Supplementary Act provides in Art 14(1) that every ECOWAS member state shall establish its own data protection authority while it provides at the same time that if any state does not have shall be encouraged to establish one. The language of 'encouragement' is not used in the Cyber Convention or in the Directive 95/46 /EC. This implies that there may be difficulties to attain harmonisation in the implementation of the Supplementary Act. The second difference rests upon the composition of the data protection authority. The Supplementary Act provides the members of the protection authority must possess qualification in the field of law, information communication technology

[1443] Greenleaf, note 1440, supra. It is important to emphasise that all of these states had adopted their data privacy legislation prior to the existence of the ECOWAS Supplementary Act. Since then to date none of the other ECOWAS member has adopted a data privacy legislation suggesting that the impact of the Supplementary Act is yet to be felt in the sub-region.

and other field of knowledge to achieve the objectives of the Act. In contrast, the Cyber Convention does not specify these qualifications expressly. It rather provides a list of persons who may serve in the protection authority as members. Although in effect those named individuals possess similar qualifications as those in the Supplementary Act, the former list other persons without specific qualifications (e.g. parliamentarians, deputies and senators). Also, it is not clear if following the appointment to serve as members of protection authority persons like senior judges listed in the Cyber Convention relinquish their original posts to the new one or they serve both. In case they maintain both posts and actually work for them, it is highly likely they may be overwhelmed by the responsibilities and fail to work efficiently. Moreover there is great likelihood of conflict of interests to arise. The third area of difference appears only as an oversight in repetition of the responsibilities of the protection authority. The Supplementary Act contains seventeen functions of the protection authority while the Cyber Convention has only fifteen. A close examination of the two sets of functions reveals that they are identical, except that the Supplementary Act makes repetition of two functions (Arts 19(1)(a) and 19(1)(c); Arts 19(1)(h) and 19(1)(q)) in its list. Yet in both cases the positive statement of the necessary qualifications of protection authority members, and the negative statement of incompatibilities, are unusual in international agreements concerning independence of DPAs.[1444]

Also, the Supplementary Act contains identical provisions on formalities for processing personal data as those provided in the Cyber Convention. These appear in chapter III (Arts 5-13). The corresponding provisions are contained in Arts II-5 to II-13 of the Cyber Convention. In both cases personal data processing is subject to a declaration before a protection authority. However this general principle is subject to a number of exceptions.

Finally, contrary to the Cyber Convention and Directive 95/46/EC, the Supplementary Act is an integral part of the ECOWAS Treaty.[1445] Breaches of the Supplementary Act by member states can be enforced before the ECOWAS Court of Justice. It is also imperative to note that neither the Supplementary Act nor the Cyber Convention provides the time limit for member states to implement them. This is in contrast to the Directive which put the duration for implementation. What it means is that the harmonisation process in ECOWAS is much more complicated. This is because, while four ECOWAS members have adopted data privacy legislation the rest have not yet done so.

[1444] Greenleaf, p.9, note 942, supra.
[1445] ECOWAS Supplementary Act 2010, Art 48.

4.4.2.2 East African Community

The East African Community comprises of five countries: Kenya, Uganda, Tanzania, Rwanda and Burundi. The Community was established in 1999 by the Treaty for Establishing of the East African Community 1999.[1446] The major aim of the EAC is to forester development among the member states. To this end, the East African Community established a Customs Union in 2005 and a Common Market in 2010.[1447] There are two instruments in EAC which relate to data privacy protection. These are considered below.

(a) Bill of Rights for the East African Community 2009

The Bill of Rights for the East African Community 2009[1448](i.e. BREAC or East African Bill of Rights) is still a draft law. It has not yet been adopted by EAC. The Bill was prepared by the Human Rights institutions in the EAC. The major objective of the Bill of Rights is to address the omissions in the national constitutions of the member states as well as harmonise the standard of protection of human rights across the sub-region.

In contrast to the African Charter on Human and Peoples' Rights which omits express reference to protection of the right to privacy, the East African Bill of Rights provides in Art 7 as follows:-

> '1. Every person has the right to privacy, which includes the right not to have-
> (a) their person, office, or home searched;
> (b) their property searched;
> (c) their possessions seized;
> (d) the privacy of their communications infringed;
> Except as authorized by law.'

[1446] The Treaty for Establishment of the East African Community was signed on 30 November 1999 and entered into force on 7 July 2000 following its ratification by the original three Partner States – Kenya, Uganda and Tanzania. The Republic of Rwanda and the Republic of Burundi acceded to the EAC Treaty on 18 June 2007 and became full Members of the Community with effect from 1 July 2007; see EAC Website, http://www.eac.int/about-eac.html last visited 12/03/2012.
[1447] Ibid.
[1448] The Draft Bill of Rights for the East African Community 2009, http://www.kituochakatiba.org/index2.php?option=com_docman&task=doc_view&gid=410&Itemid=27 last visited 12/03/2012.

The above provision differs significantly in its formulation from the corresponding provision in the international instruments such as the Universal Declaration of Human Rights 1948 and International Covenant on Civil and Political Rights 1966. It also differs from other regional instruments including the European Convention on Human Rights 1950 and even the African Charter on the Rights and Welfare of the Child 1990. These instruments protect privacy in terms of private and family life including right to honour and reputation. In contrast, the East African Bill of Rights does so in terms of unauthorised searches of the person, office, home and property. The Bill also prevents seizure of possessions and infringement of communications. It is submitted that although the provisions of the East African Bill of Rights regarding searches and seizure may have implication in the private and family life of an individual, the same are not equivalent. Yet, the provision on privacy of communications and that on correspondence in the two sets of laws may be similarly interpreted. Since the Bill is not yet adopted, it has to be waited to see how far its Art 7 will have impact once the law comes into force as it is proposed.

(b) EAC Legal Framework for Cyber Laws 2008/2011

Like other regional groupings in the world, the East African Community has not been isolated by the development of ICTs. The potential benefits and risks of using ICTs are issues which have recently gained prominent discussion in the EAC. Accordingly, the realization of a solid cyber laws regime in the Community is essential in underpinning the implementation of the Common Market Protocol especially on the services, an area of great potential for the region.[1449] Yet, the EAC cyber law reform programme began on 28 November 2006 much earlier than the beginning of Common Market Protocol. This was after the East African Community's Council of Ministers identified the creation of an enabling legal and regulatory environment as an enabling factor for effective implementation of e-Government strategies at national and regional levels.[1450]

The cyber law reform programme was preceded by the appointment of the Regional Task Force on Cyberlaws (the Task Force) established in December 2007.[1451] The latter drew from member

[1449] Dr. Enos Bukuku, the EAC Deputy Secretary General in charge of Planning and Infrastructure, see UNCTAD, Press Clipping: EAC Develops Cyber Laws, 25/10/2011, http://r0.unctad.org/ecommerce/docs/EAC_Media.pdf last visited 12/03/2012.
[1450] Ibid; see also Legal Notice No. EAC/8/2007, East African Community Gazette, Vol.AT 1-No.0004, Arusha 30th December 2007; East African Community, Draft EAC Legal Framework for Cyber Laws, (Phase I) November 2008, p.3.
[1451] EAC, Draft EAC Legal Framework for Cyberlaws, (Phase I), p.4.

states ministries and government departments.[1452] To successfully accomplish its task, the Task Force organized the reform process in two phases: Phases I and II. The criteria for this division based on the priority of issues to be addressed. Accordingly, Phase I comprised the following issues: electronic transaction, electronic signature and authentications, data protection and privacy, consumer protection and computer crimes. It is this first phase which is crucial and relevant in this thesis as it addresses privacy and data protection law issues. The second phase comprised the following issues: intellectual property, domain names, taxation and freedom of information.

The primary purpose for EAC Legal Framework for Cyber Law Framework (i.e. the Cyber Law Framework) is harmonization of policies and regulation in the sub-region. This purpose has been repeatedly emphasized in the *travaux préparatoires* of the Framework. For instance the East African Community Task Force on Cyber Laws: Comparative Review and Draft Legal Framework puts categorically:-

> 'The purpose of developing a Cyber Law Framework (Framework) for the EAC Partner States is to promote regional harmonisation in the legal response to the challenges raised by the increasing use and reliance on ICTs for commercial and administrative activities, specifically in an Internet or cyberspace environment.'[1453]

The above purpose is similarly entrenched in the Background Paper for the Second Meeting of the EAC Task Force on Cyber Laws,[1454] Report of the 2nd EAC Regional Task Force Meeting on Cyber Laws[1455] as well as the two EAC Cyber Laws Frameworks.[1456] Yet, despite this purpose, the approach embarked by EAC to achieve it has left these countries to stay far apart. The EAC Cyber Laws are termed as 'Frameworks'. However in contrast to international and other regional codes and regulations on cyber laws, and particularly in the field of privacy and data protection, the EAC Cyber Laws Frameworks do not provide any content principles as minimum standards for its members to adhere. The *travaux préparatoires* of the framework clearly points that 'the

[1452] Ibid.
[1453] Walden, I., 'East African Community Task Force on Cyber Laws: Comparative Review and Draft Legal Framework', Draft v.1.0, 2/5/08 prepared on behalf of UNCTAD and the EAC, May 2008, p.8.
[1454] EAC, Background Paper for the Second Meeting of the EAC Task Force on Cyberlaws, Golf Course Hotel, Kampala, Uganda, 23rd -25th June 2008, EAC/TF/2/2008, (Annex I), p.2.
[1455] EAC, Report of the 2nd EAC Regional Task Force Meeting on Cyberlaws, Golf Course Hotel, Kampala, Uganda, 23rd -25th June 2008, EAC/TF/2/2008, p. 6.
[1456] EAC, EAC Legal Framework for Cyberlaws, (Phase I), p.5; EAC, EAC Legal Framework for Cyberlaws, (Phase II), p.3.

Framework is not itself a model law, thereby focusing the debate within the Task Force on the nature of the provisions being recommended to Partner States and avoiding the need for detailed scrutiny of specific draft provisions.'[1457] The rationale for adopting this approach is twofold: to accommodate the progress of the law reform process already underway within certain Partner States and also it is pragmatic response to the work that has already been carried out in various forums and intergovernmental organizations, which obviates the need to reinvent the wheel in each topic area.[1458] In this regard, the EAC Cyber Laws Frameworks have taken an approach of only making recommendations to member states. Such recommendations are not intended to be binding but for member states to take into account when enacting cyber laws in their countries.

As pointed out, EAC Legal Framework for Cyber Law (Phase I) is the relevant Framework in the field of data protection. Its preparation was preceded by three important meetings of the Task Force. The first meeting took place in Arusha, Tanzania on 28-30 January 2008. The second took place in Kampala, Uganda on 23-25 June 2008 and the third meeting was held in Bujumbura, Burundi on 10-11 September 2008. During these meetings, the EAC member states reviewed the status of cyber laws in their respective countries. They also deliberated specific areas which needed reforms. Professor Ian Walden, Head of the Institute of Computer and Communications Law, Queen Mary, University of London, was hired as consultant. Initially the final draft legal cyber law framework was scheduled to be considered and adopted by the relevant organs of the EAC by November 2008.[1459] Member states were to enact cyber laws by 2010.[1460] However, it was until 7 May 2010 when the EAC Cyber Law Framework (Phase I) was adopted by the 2nd Extra-Ordinary Meeting of the Community's Sectoral Council on Transport, Communications and Meteorology.[1461] The Council urged member states to make use of the EAC Legal Framework for Cyber Law Phase I, particularly when initiating related policies and laws.[1462] It also directed the Secretariat to develop a monitoring system and report on the implementation of the recommendations of EAC Legal Framework for cyber laws.[1463]

In the field of data privacy law the *travaux préparatoires* recommended two minimum obligations should be imposed with regard to a processing activity. First, is to comply with certain 'principles

[1457] Walden, p.9, note 1453, supra; EAC, EAC Legal Framework for Cyberlaws, (Phase I), p.6.
[1458] Ibid.
[1459] EAC, p.4, note 1455, supra.
[1460] Ibid.
[1461] EAC, The 2nd Extra-Ordinary Meeting of the EAC Sectoral Council on Transport, Communications and Meteorology: Report of the Meeting, EAC/SR/2010, Para 2.2(b).
[1462] Ibid, Para 2.2(c).
[1463] Ibid, Para 2.2(e).

of good practice' in respect of their processing activities, including accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security.[1464] Second, is to supply the individual with a copy of any personal data being held and processed and provide an opportunity for incorrect data to be amended.[1465] The preparatory works also cautioned about cost for implementing comprehensive data privacy laws in EAC. This caution provides:-

> 'The cost of regulation will be a critical factor in data protection. The cost associated with a comprehensive or omnibus approach, specifically the establishment of a dedicated regulatory authority, will generally be excessive for most developing countries, especially if borne by the private sector through licensing or notification fees. However, in terms of addressing privacy concerns vis-à-vis public sector infringements, an authority independent from government will generally be necessary in order to provide the necessary trust and assurance in its activities. The regulatory authority may not have an exclusive data protection remit, which mitigates the costs involved.'[1466]

The above minimum obligations regarding data processing as well as the caution about cost for implementing comprehensive data privacy law are repeated in the EAC Cyber Law Framework (Phase I) itself.[1467] Accordingly, the Cyber Framework incorporates Recommendation 19 which states:-

> 'The Task Force recognises the critical importance of data protection and privacy and recommends that further work needs to carried (sic) on this issue, to ensure that (a) the privacy of citizens is not eroded through internet; (b) that legislation providing for access to official information is appropriately taken into account; (c) the institutional implications of such reforms and (d) to take into account fully international best practice in the area (R.19).'[1468]

While R 19 recommends to the EAC member states to take into account 'fully' international best practice in the area it avoids mention of any of such best practices. Moreover, the EAC Cyber Law Framework (Phase I) has avoided to attach any annex of international code on data privacy

[1464] Walden, p.17, note 1453, supra.
[1465] Ibid.
[1466] Ibid, pp.17-18.
[1467] EAC, EAC Legal Framework for Cyberlaws, (Phase I), pp. 17-18.
[1468] Ibid, p.18; see also, Annex I, R. 19 to the EAC, EAC Legal Framework for Cyberlaws, (Phase I).

as it has been the case with other areas addressed in the Framework: electronic transaction, electronic signature and authentications, consumer protection and computer crimes. This omission may have adverse implication in achieving harmonization of data privacy law in the sub-region. The reason is simply that each member may opt to follow one 'international best practice' different from the other. It is submitted that the Framework has not yet produced any tangible impact in the data privacy reforms in East Africa. This point is correctly observed by Greenleaf:-

> 'Less advanced as yet, the East African Community (EAC), a regional group of five East African countries (Kenya, Tanzania, Uganda, Rwanda and Burundi) has taken various initiatives that encourage the member states to adopt data privacy legislation. Such initiatives include the current discussion of *A Draft Bill of Rights for the East African Community* which unlike the African Charter on Human and Peoples' Rights incorporates the right to privacy. Also, although not binding, the EAC has adopted *EAC Framework for Cyberlaws* Phases I and II in 2008 and 2011 respectively, addressing multiple cyber law issues including data protection. Yet as of now only Kenya is considering a draft bill on data protection.'[1469]

Worthwhile to mention, the draft data privacy Bill in Kenya was developed much earlier than the adoption of the EAC Legal Framework for Cyber Law (Phase I). The initial draft of the Data Protection Bill was published by the Kenyan Ministry of Information and Communication in June 2009. There is therefore little evidence to link directly the outcome of this draft to the EAC cyber law reform programme. Yet currently Kenya has a new version of the draft data privacy Bill, the Data Protection Bill 2012. The latter version partly came about as a result of the adoption of the new Kenyan Constitution in 2010 (incorporating the right to privacy for the first time) as well as strong criticisms particularly from the ARTICLE 19.[1470] The main criticisms of ARTICLE 19 to the Kenyan draft Data Protection Bill 2009 are as follows. First, the Bill only applies to personal information held by public authorities. The private sector remains unregulated. Second, although the Bill uses the term 'personal information' it fails to limit the application of the law in cases where public servants are conducting business. Third, some concepts are included in the definitions but are not further mentioned in the text (e.g. public servants, whistleblowing and public records). Fourth, the Bill does not provide for additional

[1469] Grenleaf, (Global Data Privacy Law: 89 Countries and Accelerating), pp. 7-8, note 38, supra.
[1470] ARTICLE 19, note 1335, supra.

funding of the Information Commission which will take charge of both the data privacy and freedom of information law.

The cyber law reform programme has a number of implications. First, the programme purports to achieve harmonization of data privacy policies and laws in the sub-region without spelling out minimum standards for EAC member countries to adhere. Surely this is a significant departure from its counterpart ECOWAS sub-region. The latter has imposed binding minimum standards of data protection principles and establishment of a data protection authority on its member states. This is also the case with the current proposed African Union Cyber Convention. Similarly, the East African Community's approach to data privacy protection is found nowhere in the world. Second, while cost implications for implementing data privacy law are critical, the overemphasis on such cost put by the reform programme in relation to the adoption of comprehensive data protection laws may have far reaching ramifications for EAC readiness to reform. Third, there is virtually little expertise in the field of data privacy in the sub-region. This situation compelled the EAC to engage a consultant from the United Kingdom. Yet such consultant could not meet the entire demands for expertise in the sub-region. Linked to expertise is the issue of funding the reforms in individual member state. This point is clearly illustrated by the representative from Burundi in the Task Force, Mr. Gabriel Bihumugani as reported in the proceedings of the Task Force:-

> 'Commenting on the draft legal frame work, the delegate informed members that the Government of Burundi had not yet drafted any bill on cyber laws. It was noted that due to constraints of time, finances and expertise, Burundi was not in a position to organize a National Consultative Workshop. Therefore the Burundi delegation requested for help in terms of a technical expert (consultant) and funding for a National Consultative Workshop on cyber laws so as to move faster and in harmony with other sister EAC partner states.'[1471]

Fourth, the cyber law reform in EAC identified little awareness of cyber laws by calling for sensitization workshops for parliamentarians.[1472] The rationale for that was/is to accelerate the process of enacting cyber laws in the sub-region. Similarly, the reform programme identified capacity building to judges, law researchers, legal practitioners and other officers involved in the

[1471] ECA, pp.4 and 13, note 1454, supra.
[1472] Ibid, p.13.

implementation of the proposed cyber laws as necessary.[1473] It is submitted that these factors have to some extent contributed to the slow legislative reforms in the sub-region.

4.4.2.3 Southern African Development Community

The Sothern African Development Community (SADC) is a sub-regional grouping of fifteen countries: Angola, Botswana, Democratic Republic of the Congo (DRC), Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe. Originally known as the Southern African Development Co-ordination Conference (SADCC), the organisation was formed in Lusaka, Zambia on 1 April 1980, following the adoption of the Lusaka Declaration. The Declaration and Treaty establishing the Southern African Development Community[1474] (SADC) which has replaced the Co-ordination Conference was signed at the Summit of Heads of State or Government on 17 August 1992, in Windhoek, Namibia.[1475]

Initially the members of SADC came together as *Frontline States* whose objective was political liberation of Southern Africa. However SADC's objectives have since then been significantly expanded to include the following: achieve development and economic growth, alleviate poverty, enhance the standard and quality of life of the people of Southern Africa and support the socially disadvantaged through regional integration; evolve common political values, systems and institutions; promote and defend peace and security; promote self-sustaining development on the basis of collective self-reliance, and the interdependence of Member States; achieve complementarity between national and regional strategies and programmes; promote and maximise productive employment and utilisation of resources of the Region; achieve sustainable utilisation of natural resources and effective protection of the environment; strengthen and consolidate the long standing historical, social and cultural affinities and links among the people of the Region.[1476] In order to achieve these objectives, one of the strategies adopted by SADC is to harmonise political and socio-economic policies and plans of Member States.[1477]

[1473] Ibid.
[1474] Declaration and Treaty of SADC as revised in 1992, http://www.sadc.int/index/browse/page/119 last visited 16/03/2012.
[1475] SADC, Website, http://www.sadc.int/english/about-sadc/ last visited 16/03/2012.
[1476] Declaration and Treaty of SADC, Art 5(1).
[1477] Ibid, Art 5(2)(a).

As far as privacy and data protection is concerned only three SADC's member states namely Seychelles, Mauritius and Angola have adopted comprehensive data privacy legislation in 2003, 2004 and 2011 respectively. South Africa is still debating the Bill on data privacy law. The rest of the SADC's countries have yet adopted such laws. However, as a sub-region, SADC is currently considering to adopt a model law on data protection in the sub-region.[1478] It is imperative to highlight the SADC Data Protection Model-Law[1479] (i.e. the Model-Law) in order to compare and contrast it with other African regional and sub-regional frameworks. Also important, is to point out to what extent is it influenced by the European Directive 95/46/EC.

The Model-Law considered here is the draft version of 6 February 2012. This draft Model-Law incorporates the basic principles of data processing as well as establishment of data protection authorities in member states. As a result, it can be submitted that it is similar to the European Directive 95/46/EC. Moreover the Model-Law is similar to the AU Cyber Convention 2011 and the ECOWAS Supplementary Act 2010. Yet, there are significant differences in scope and ambit for some of the principles covered in these sets of laws. This part considers in a considerable degree these differences more than their similarities.

Structurally, the Model-Law has a preamble and fourteen chapters. In contrast to the Directive 95/46/EC, AU Cyber Convention and ECOWAS Supplementary Act, the preamble of the SADC Model-Law does not contain recitals. It rather provides broad elaboration on the nature, purpose and function of data privacy policies and laws. The problem which arises here is that while normally a preamble somewhat serves as an interpretative aid of the substantive principles to a text this may not be the case in the SADC Model-Law.

Chapter 1 of the Model-Law contains various definitions used in the text of the law. Most of the concepts are similar to the other instruments. However, the Model-Law introduces new definitions such as genetic data, transborder flow and whistleblowing. Genetic data is defined in the Model-Law as any information stemming from a DNA analysis.[1480] The Directive 95/46/EC does not contain this definition. However this omission is cured in the proposed General Data

[1478] The last workshop in which the SADC Legal Cyber Security Framework(of which data protection is a component) was under discussion was held on 27 February-2 March 2012 in Gaborone, Botswana, http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2012/Agenda.pdf last visited 16/03/2012.
[1479] SADC Data Protection Model-Law 2012, http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/sa-4.html last visited 16/03/2012.
[1480] SADC Model-Law 2012, Art 1(8).

Protection Regulation 2012.[1481] Yet, there is significant departure in the formulation. The Regulation defines genetic data as all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development. The AU Cyber Convention and ECOWAS Supplementary Act do not either contain definition of genetic data. The Directive, Cyber Convention and Supplementary Act omit a definition of the concept transborder flow. This concept is clearly explained in the contents of the texts. The only innovation brought about in the SADC Model-Law is the clarification for treating flow of personal information between federated states or between federated state and federated entities within the same federal state. In both cases, flow of personal information is not considered as transborder flow.[1482] The definition of whistleblowing is absent in the other three instruments. This is perhaps because whistleblowing are ordinarily governed by specific pieces of legislation other than data privacy legislation. Other definitions in the Model-Law such as data controller's representative are specifically referred in the text of the Directive, Cyber Convention and Supplementary Act.

In contrast to the European Directive, Cyber Convention and Supplementary Act, the Model-Law does not define its objective. Yet the protection of an individual's right to privacy as well as harmonisation of data privacy policies and laws appears to be generally implied in the preamble of the Model-Law.

The Model-Law sets out the scope of its application in chapter 2. Like the Directive, Cyber Convention and Supplementing Act, the Model-Law applies to both automatic and non-automatic processing of personal data.[1483] It also applies to both private and public data controllers.[1484] However, there is no clear provision which leaves possibilities for protection against legal persons as it is the case with the Directive or Cyber Convention and Supplementary Act. The latter two instruments leave margins for the national laws to offer protection to legal persons. The scope of the application of the Model-Law also relates to the territory. In contrast to the Cyber Convention and Supplementary Act which apply to the processing of personal data within the members of African Union and ECOWAS respectively, the Model-Law has a broader scope similar to Art 4 of the Directive 95/46/EC. Article 3(1) of the Model-Law provides:-

> 'This Model-Law is applicable:-

[1481] EU General Data Protection Regulation 2012, Art 4(10).
[1482] SADC Model-Law 2012, Art 1(17).
[1483] Ibid, Art 2(1).
[1484] Ibid, Art 1(3).

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

(b) to the processing of personal data by a controller who is not permanently established on[given country] territory, if the means used, which can be automatic or other means located on [given country] territory, are not the same as the means used for processing personal data only for purposes of transit of personal data through[given country] territory.'

The Model-Law provides further that in the circumstances referred to in the previous paragraph, the controller shall designate a representative established on [given country] territory, without prejudice to the legal proceedings that may be brought against the controller himself.[1485] Since Art 3 of the Model-Law is similar to Art 4 of Directive 95/46/EC, the analyses made on the latter in 3.3.1.6 (e) with regard to applicable law are relevant in the understanding of the ambit of the former. However it is worthwhile to note that the European Union proposed Regulation has significantly modified Art 4 of the Directive.[1486]

By way of derogation, the Model-Law does not apply to the processing of personal data by a natural person in the course of purely personal or household activities.[1487] This is similar to the application of the Directive, Cyber Convention and Supplementary Act. Additional limitations on the scope of Model-Law are provided in chapter 11 which incorporates only Art 46. Under this provision, SADC's member states are permitted to limit certain obligations put in the Model-Law. Such limitations may apply where it is necessary to preserve state security, defense, public safety, prevention, investigation, prosecution or execution of criminal sentences. Also the

[1485] Ibid, Art 3(2).
[1486] See Art 3 of the General Data Protection Regulation 2012, which states: - '1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.'
[1487] SADC Model-Law 2012, Art 2(2).

limitations apply in matters of literary and artistic expression as well as professional journalism, according to the ethical rules of this profession.

Chapters 3, 4 and 5 of the Model-Law contain the basic principles and condition for processing personal data. These principles are generally similar to those provided in the Directive, Cyber Convention and Supplementary Act. They include the following principles:-fair and lawful processing; purpose specification; legitimacy; sensitivity; data quality; security; and accountability.

Apart from containing some basic principles of data processing, chapter 5 of the Model-Law contains the obligations imposed on data controllers. Most of these obligations are formulated closely to the provisions of the Directive rather than the Cyber Convention and Supplementary Act. These obligations include provision of information prior to processing; confidentiality; security; notification of the processing to the data protection authority; and accountability. It is important to point out that some of these obligations are broader in the Model-Law than in the Cyber Convention and Supplementary Act. For example, the Model-Law imposes an obligation on the data controller to provide certain information to the data subject prior to processing. At the same time it imposes similar obligation on data controllers when personal data is not directly collected from the data subject.[1488] The Cyber Convention and ECOWAS Supplementary Act omit a provision imposing duty in the latter case.

Chapter 6 of the Model-Law provides for the rights of the data subject. These are similar to the rights provided in the Directive, Cyber Convention and Supplementary Act. They include right of access; right of rectification, deletion, temporary limitation of access; right of opposition; and representation of the data subject who is under age.

Like the Directive, Cyber Convention and Supplementary Act, the SADC Model-Law contains rules for transboder flows.[1489] Yet in contrast to the other instruments, the Model-Law contains rules which prohibit transfer of personal data not only to a non-SADC member but also to a SADC member state which has not adopted the Model-Law.[1490] Arguably the restriction in the latter case defeats the harmonisation object. Yet, this requirement may motivate SADC member states to adopt data privacy legislation in line with the Model-Law.

Chapter 7 of the Model-Law provides for the establishment of protection authority in member states. It further provides for the composition, functions and powers, sanctions and remedies for

[1488] Ibid, Arts 14 and 15 respectively.
[1489] Ibid, Chapter 12.
[1490] Ibid, Arts 47 and 48.

breaches of the provisions of the Model-Law. Generally, the rules governing the DPA in the Model-Law are similar to those in the Directive, Cyber Convention and Supplementary Act. However in contrast to the Cyber Convention and Supplementary Act, the Model-Law leaves to the member states to legislate on the incompatibility to the composition of the DPAs.[1491] Yet the Model-Law clearly puts that members of DPAs are permanent.[1492] Because of this, members of DPAs may be drawn from the executive branch of the government.[1493] Also important to note is that DPAs are required to be composed by substitute members who replace permanent members when they are absent or when mandate becomes vacant.[1494]

4.4.2.4 Other Sub-Regional Frameworks

Besides ECOWAS, EAC and SADC the other sub-regional organizations in Africa notably COMESA, ECCAS and UMA have virtually undeveloped initiatives towards adoption of data privacy legislation. However some states in these sub-regional groupings have already adopted data privacy legislation. This is the case with Tunisia and Morocco which are members of the Arab Maghreb Union (with its French acronym UMA).

4.4.3 National Frameworks

As pointed out in 1.2.1, there are three main patterns of protection of data privacy at national level in Africa. The highest order of such protection is the national constitution of a respective country. Within this category various sub-patterns may be identified. There are countries whose constitutions contain express provisions for protection of privacy. This is the dominant pattern. Yet, there are various formulations of the right to privacy with different scope and ambit. For example, Art 37 of the Constitution of Federal Republic of Nigeria 1999 states, 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'. This provision only affords privacy protection to citizens. A resident or non-citizen cannot claim protection for privacy under the Nigerian Constitution. Accordingly, the Nigerian Constitution provides a narrow scope of privacy protection. Kenya provides somewhat broader scope of protection. Art 31 of the Constitution of Kenya 2010 provides, 'every person has the right to privacy, which includes the right not to have (*a*) their person, home or property searched; (*b*) their possessions seized; (*c*) information relating to their

[1491] Ibid, Art 33(3).
[1492] Ibid, Art 33(1).
[1493] Ibid.
[1494] Ibid, Art 33(1).

family or private affairs unnecessarily required or revealed; or (*d*) the privacy of their communications infringed.' This provision starts by the expression 'every person' as against 'the privacy of citizens' in the Nigerian Constitution. In the former a citizen and a non-citizen may be afforded privacy protection under the Kenyan Constitution. Also, it can be noted from the contents of these two privacy provisions that there are significant departures. Yet, judicial interpretation may make these provisions at equal level despite their variations in wordings and expressions. Currently this case law is scant (e.g. South Africa) or lacking in some jurisdictions. There are other countries whose constitutions are silent on privacy protection. Included in this category is Zimbabwe. However, Zimbabwe's proposed new constitution has an express provision on privacy protection. Worthwhile to point out, some constitutions maintain two sets of provisions for protection of privacy. The first set relates to similar protection as entrenched in the international and regional instruments protecting human rights: the UDHR, ICCPR, ECHR, ACRWC, etc or sometimes with limited provisions to communications only. The second set is *habeas data*. Cape Verde is illustrative. Article 44 of the Constitution of the Republic of Cape Verde 2010 provides that the privacy of correspondence and telecommunications are to be guaranteed to all citizens. The same Constitution provides in Art 46(1) for the right of *habeas data*. Moreover, the Constitution of Cape Verde provides another unique constitutional pattern with respect to privacy protection which is absent in many African states' constitutions. Article 45(1) of the Cape Verdean Constitution provides that all Cape Verdean citizens have the right to access data which concern them, to demand that such data be corrected and updated, as well as the right to be informed of the purposes to which these data are being put.[1495] Art 45(2) forbids the use of computerized means to store and process individually identifiable data relating to the political, philosophical, or ideological convictions, religious faith, party, or union affiliation and private life of citizens.[1496] Art 45 includes restrictions to the right of public authorities and other institutions to transfer citizens' personal data to other authorities and institutions to those cases provided for by law or judicial order; prohibition from the Cape Verdean government from attributing a uniform identification number to its citizens; and a statement indicating that the legislator is to implement a legal regime in order to regulate the cross-border transfer of data.[1497]

As a basis for protecting privacy, a constitutional right to privacy has three limitations. First, the scope of the constitutional right to privacy depends on courts' interpretation on a case to case

[1495] English translation of Art 45 of the Cape Verdean Constitution 2010(original in Portuguese language) adopted from Traca, and Embry, p.2, note 38, supra.
[1496] Ibid.
[1497] Ibid.

basis. This makes the law uncertain until actual case has been filed in court. Secondly, in most cases constitutions only protect against infringements of privacy committed by the state and its agencies. The private sector is excluded. Since the private sector is fast growing and expanding in Africa constitutional protection does not prevent misuse of personal information by businesses and private sector entities. Thirdly, infringements of constitutional right to privacy attract different remedies from those obtained under data protection legislation. For example, monetary compensation has never been a remedy under breaches of constitutional provisions.

Apart from the constitutional protection, there are also statutory protections. These are either by comprehensive data privacy laws, sectoral laws or *ad hoc* provisions in different statutes. The main manifestations of sectoral law protecting privacy are those in the communications sector, health and employment. However in most cases these sectoral laws fail to address specific principles in that relevant sector. This is the case, for example, of the employment sector and the requirements of mandatory or concealed pre-employment HIV/Aids test by employers. In case of *ad hoc* provisions, the laws contain only few sections which may have privacy implication.

There is finally protection of privacy through common law. Yet, this form of protection is clearly available in few African countries (e.g. South Africa). Currently South Africa is the only African jurisdiction which has relatively large corpus of case law on common law privacy.

4.5 Conclusion

The preceding analyses safely lead to inescapable conclusions that privacy is an evolving concept in Africa. Yet there is currently no specific way or theory which explains privacy in the context of African culture. This is partly because the notion of privacy is a Western individualist concept. It was only imported to Africa through external contacts with Europe. As a result individuals' attitudes to privacy are slowly being shaped and reshaped by Western influence. While there are at present no surveys which have attempted to precisely test the attitudes to privacy, the recent awareness survey of data protection legislation in Africa suggests that Africans' attitudes to privacy are largely limited by lack of awareness of what is privacy and implications which follow in case of privacy infringement. However the positive and negative determinants of privacy concerns continue to accelerate the understanding of the privacy concept and its infringement. While these concerns have not so far influenced to a considerable extent the recent adoption of data privacy legislation in some African jurisdictions, they are likely to support the application of

such laws. The fact that the existence of data privacy policies and legislation in Africa are directly influenced by Arts 25 and 26 of the European Directive 95/46/EC on account of restrictions the latter impose on transfer of personal data to third countries and the economic justification theory, may not render these laws wholly ineffective and irrelevant. Analogously argued, the current constitutions in African countries which have generated corpus of case law on protection of individuals' rights other than privacy were adopted with significant influence from outside. Nonetheless, individuals are basing their claims to protect their individual rights. However, it has to be seen to what extent the newly adopted data privacy policies and legislation are going to be effective. There is yet a problem of harmonization. Different data privacy policies and regulations are being adopted in Africa. These cut across regional, sub-regional and national levels. So far the full impact of these instruments is difficult to assess as they are still evolving or put in limited practices. Yet, the disparities in these instruments have/will have far reaching consequences on harmonization.

5. Data Protection in Mauritius

5.1 Introduction

Mauritius is the first case study of the present research. In contrast to the other two cases (i.e. South Africa and Tanzania); she has comprehensive data privacy protection legislation. This chapter analyses the Mauritian data protection system. The analyses commence with the context in which the Mauritian data protection sytem developed. By context it means the socio-economic and political environment. Subsequently, the analysis of the policies and regulations governing data protection is offered. Particular focus is placed upon the Mauritian data privacy legislation. Sectoral legislation as well as legislation incorporating *ad hoc* provisions relevant to data protection are left unexamined in detail. This exclusion owes largely to the fact that, such legislation does not contain the basic principles of data processing. Likewise, the analysis of the data protection legislation is relevant to the sectoral legislation and statutes with *ad hoc* provisions on data protection. Moreover the latter pieces of legislation provide no central authority to implement legislation similar to the one provided under the data protection legislation. Finally, this chapter canvasses practices of the data protection authority. Matters included in the list of practices are general supervisory role, development of codes of conduct, various decisions of the authority, etc.

5.2 Socio-Economic and Political Context

The Republic of Mauritius consists of an island of Mauritius and other three smaller islands of Rodrigues, Cargados Carajos and Agalega. Mauritius lies east of Madagascar (an island to the south-eastern Africa), in the Indian Ocean. It occupies a total area of 2,040 square kilometres. The capital of Mauritius is Port Louis. Mauritian total population as recorded by the 2011 Housing and Population Census is 1,257,900.[1498] Out of this population 42 per cent lives in the urban areas with the largest population of 149,000 in Port Louis while the rest still lives in the rural areas.[1499]

[1498] Mauritius, Housing and Population Census 2011, http://www.gov.mu/portal/goc/cso/ei915/esi2011.pdf last visited 17/03/2012.
[1499] CIA., 'Mauritius People 2012' World FactBook and Other Sources 2012, http://www.theodora.com/wfbcurrent/mauritius/mauritius_people.html last visited 17/03/2012.

Noteworthy, the above population consists of descendants of original immigrants from India, Europe, Madagascar, Africa and China. These immigrants have resulted into the following ethnic groups in Mauritius: Indo-Mauritian (68%), Creole (27%), Sino-Mauritian (3%) and Franco-Mauritian (2%).[1500] Concomitantly, loyalties usually lie with specific ethnolinguistic groups rather than the nation as a whole.[1501] Yet, there is unity. However, these diversities are also reflected in the languages used in Mauritius. Such languages are English, French, Creole, Bhojpuri and other smaller groups of languages. Although there is no clear policy as which language is the national language, English is the official language. Its domain includes medium of instruction in schools, official language of politics, judiciary, parliament and administration.[1502] Yet, it is only spoken by less than 1% of the population in Mauritius.[1503] Interestingly, Creole is dominantly spoken in Mauritius by 80.5% of the population. Next to Creole is Bhojpuri (12.1%), French (3.4%), others (3.7%) and unspecified (0.3%).[1504]

There are four main religions in Mauritius. The dominant religion is Hindu (48%).[1505] Hinduism has its origin from India. Christianity is the next largest religion in Mauritius. It comprises of Roman Catholic (23.6%) and other Christian denominations (8.6%).[1506] Muslims constitute 16.6% while other religions 2.5%.[1507] There is yet unspecified religions which constitute 0.3%. The last group is of people with no religion (0.4%).[1508] None of these religions is a state religion making Mauritius a secular state.

Politically, Mauritius is a multi-party system and constitutional parliamentary democracy with the president as head of state and prime minister as head of government. The Constitution is the supreme law in Mauritius and if any other law is inconsistent with it, that other law, to the extent

---

[1500] Ibid.
[1501] Carrim, A.J., 'Use and Standardisation of Mauritian Creole in Electronically Mediated Communication', Journal of Computer-Mediated Communication, 2009, Vol.14, No.3, pp.484-508, at p.484.
[1502] CIA, note 1499, supra; see also Mahadeo, S.K., 'History of English and French in Mauritius: A Study in Language and Power', International Journal of Language, Society and Culture, 2004, Issue No.14, http://www.educ.utas.edu.au/users/tle/journal/articles/Mahadeo/Mahadeo4.html, last visited 17/03/2012; Mahadeo, S.K., 'English Language Teaching in Mauritius: A Need for clarity of vision regarding English Language Policy', International Journal of Language, Society and Culture, 2006, Issue No.18, http://www.educ.utas.edu.au/users/tle/journal/articles/2006/18-2.htm last visited 17/03/2012.
[1503] CIA, note 1499, supra; see also Carrim, note 1501, supra; Carrim, A.R., 'Language Use and Attitudes in Mauritius on the Basis of the 2000 Population Census', Journal of Multilingual and Multicultural Development, 2005, Vol. 26, No.4, pp.317-332, at pp.319-329.
[1504] Ibid.
[1505] CIA, note 1499, supra.
[1506] Ibid.
[1507] Ibid.
[1508] Ibid.

of inconsistency, becomes void.[1509] According to reports by the Democracy Index (2007, 2008, 2010 and 2011) Mauritius is the only African country which is characterised as fully democracy equating it with most developed countries in Europe.[1510]

Mauritius attained her political independence from the British on 12 March 1968. However she continued to be under her Majesty the Queen of England as head of State until 12 March 1992 when she became a Republic. Prior to independence Mauritius had witnessed the influence of the Arabs, Dutch, Chinese and French. However the French had the most influence and legacy in the Island. Although the French activities in Mauritius commenced in 1715, it was until the 1767 when the French governance started. The French domination in Mauritius ended in 1810 following their defeat by the British in the Napoleonic War. Subsequently, the British took control of Mauritius until 1968.

The British influence in Mauritius accounts for the Mauritian legislative system. The latter is modelled after the Westminster system of parliamentary democracy which was common in most British colonies during independence. The legislature consists of the President and a National Assembly.[1511] The latter which is commonly referred to as Parliament consists of 70 elected members.[1512] The political party or party alliance which wins the majority of seats in Parliament forms the government and its leader usually becomes the Prime Minister.[1513] The judicial system is similarly influenced by the British characterised by the adversarial system of litigation and precedent. The Constitution establishes the Supreme Court of Mauritius at the apex of the judicial hierarchy and vests it with unlimited jurisdiction in both criminal and civil matters.[1514] However under Art 81 of the Constitution of Mauritius all appeals from the Supreme Court lie

[1509] The Constitution of Mauritius 1968, Art 2.
[1510] The Economist Intelligence Unit's Index of Democracy 2007,
http://www.economist.com/media/pdf/DEMOCRACY_INDEX_2007_v3.pdf last visited 17/03/2012;
The Economist Intelligence Unit's Index of Democracy 2008,
http://graphics.eiu.com/PDF/Democracy%20Index%202008.pdf last visited 17/03/2012;
The Economist Intelligence Unit's Index of Democracy 2010,
http://graphics.eiu.com/PDF/Democracy_Index_2010_web.pdf last visited 17/03/2012;
The Economist Intelligence Unit's Index of Democracy 2011,
http://www.eiu.com/Handlers/WhitepaperHandler.ashx?fi=Democracy_Index_Final_Dec_2011.pdf&mode=wp,
last visited 17/03/2012. It is imperative to note that the Economist Intelligence Unit uses five criteria for its assessment: electoral process and pluralism; civil liberties; the functioning of government; political participation; and political culture. Moreover, countries are placed into four types of regimes: full democracy; flawed democracy; hybrid regimes; and authoritarian regimes. Although democracy as a concept is still problematic to define, these reports provide some highlights useful to situate a given country.
[1511] The Constitution of Mauritius 1968, Art 31(1).
[1512] Ibid, Art 31(2).
[1513] Mauritius, National Assembly Website,
http://www.gov.mu/portal/site/AssemblySite/menuitem.37a73b08329da0451251701065c521ca/
last visited 18/03/2012.
[1514] The Constitution of Mauritius 1968, Art 76.

to the Privy Council in the Great Britain. Below the Supreme Court there are subordinate courts: the District Courts, Intermediate and Industrial Courts. These are vested with limited jurisdictions in criminal and civil matters. Yet the influence of the French law is also present in the Mauritian legal system. This makes Mauritius to have a hybrid legal system with the influence of the British and French laws. In general terms, Mauritian private law is based on the French *Code Civil* while public and commercial law are based on the English law.[1515]

The Mauritian economy has undergone remarkable transformations since independence to the extent that it is now characterised by the World Bank as an upper-middle economy.[1516] After independence, Mauritius continued to rely upon sugar export as a primary source of its economy. Sugar plantations were introduced by the French in the Island during their domination. Yet in early 1970s Mauritius directed its efforts to diversify its economy which efforts proved failure by late 1970s.[1517] This failure was attributed by rising of petroleum prices, ending of the sugar boom, and the steadily rising of the balance of payments as imports outpaced exports.[1518] To address the economic crisis Mauritius approached the IMF and World Bank for assistance,[1519] a situation which was common to many other African countries in1970s-1980s. In exchange for loans and credits the Mauritian government agreed to institute certain measures, including cutting down food subsidies, devaluing the currency, and limiting government wage increases.[1520] Built partly on these measures conditioned by SAPs and other subsequent initiatives, Mauritius managed to diversify its economies. Today, agriculture, textile manufacturing, tourism and financial services account for Mauritius economic sectors. Moreover, since 2000s Mauritius started to invest significantly in ICT as the fifth pillar of the country's economy.[1521] Yet, the ICT sector is also intended to drive other sectors of the Mauritian economy. In order to ensure that this sector

---

[1515] Brown, L. N., 'Mauritius: Mixed Laws in a Mini-Jurisdiction', in Örücü, E (eds), et al., Studies in Legal Systems: Mixed and Mixing, Kluwer International, London, 1996, pp.210-214, at 218 cited in Bridge, J.W., 'Judicial review in Mauritius and the Continuing Influence of English Law', International and Comparative Law Quarterly, 1997, Vol.46, No.4, pp.787-811, at p. 787.

[1516] Metz, H.C(ed)., Mauritius: A Country Study, GPO for the Library of Congress, Washington, 1994, http://countrystudies.us/mauritius/ last visited 18/03/2012; see also World Bank List of Economies(July 2010), http://www.fas.usda.gov/mos/em-markets/World%20Bank.pdf,
Last visited 18/03/2012; see also, World Bank List of Economies(18 July 2011),
http://shop.ifrs.org/files/CLASS.pdf last visited 18/03/2012.

[1517] Metz, note 1516, supra.

[1518] Ibid.

[1519] Ibid.

[1520] Ibid.

[1521] See e.g., Mauritius Research Council., Information & Communications Technology Report, 2001, http://www.mrc.org.mu/Documents/Thematic/ICTReport.pdf last visited 18/03/2012; National ICT Strategic Plan (NICTSP) 2007-2011,
http://unpan1.un.org/intradoc/groups/public/documents/cpsi/unpan030903.pdf,
last visited 18/03/2012;
National ICT Strategic Plan (NICTSP) 2011-2014, http://www.gov.mu/portal/goc/telecomit/file/ICTplan.pdf last visited 18/03/2012.

grows rapidly and produce desired results, Mauritian legislature passed the Information and Communication Technologies Act 2001.[1522] Similarly, in 2007 Mauritius adopted its first National Information and Communications Technology (ICT) Policy 2007.[1523] ICT use and access in Mauritius is becoming common in households.[1524] In 2011, the proportion of households having mobile phones was 88.2% up from 28.1% in 2001; computers was 37.6% up from 13.3% in 2001; and internet was 31.7% up from 12.6% in 2002.[1525]

Internationally, Mauritius is a member of various intergovernmental organisations: the United Nations (UN), African Union (AU), SADC and COMESA. This implies that Mauritius is under certain international obligations. These include, for example, obligation to implement resolutions and agreements flowing from those organisations she is a member.

5.3 Social Attitudes to Privacy

There have been no major and general academic, government or industry studies or surveys on privacy in Mauritius. As a result it is difficult to provide a general level of privacy attitude by Mauritians. Nonetheless, there exist specific studies which are privacy relevant. While these do not provide a general survey, they offer a snapshot of privacy concerns in Mauritius. The first of these studies was conducted in the context of the adoption of Internet banking in Mauritius. It found that although banks have security arrangements such as network and data access controls, user authentication, transaction verification, virus protection, privacy policies and detection of possible intrusions which include penetration testing, intrusion detection, etc raised customers' concerns on possible risks from Internet banking.[1526] The debates over the legislative process of the Mauritian DNA Identification Act 2009 present yet another context of concern for privacy in Mauritius.[1527] These debates rested on both privacy and ethical issues. First, the adoption of the Act resulted in heated debates between the government and the opposition party over retention of DNA samples once the case is over. Second, the debates raged over who should carry out analyses of DNA samples. Was this to be done by private, independent or by government laboratories? The government argued that DNA samples should be collected and

[1522] Act No.44 of 2001.
[1523] Ministry of Information Technology and Telecommunications National ICT Policy 2007-2011, http://www.ist-africa.org/home/files/Mauritius_ICTPolicy_2007-11.pdf last visited 18/03/2012.
[1524] Mauritius, note 1498, supra.
[1525] Ibid.
[1526] Khan, N.M and Emmambokus, N., 'Customer Adoption of Internet Banking in Mauritius', International Journal of Business Research and Management(IJBRM), 2011, Vol.2, No.2, pp.53-58, at p.56.
[1527] See e.g. Maurer, S., 'Genetic Identity in Mauritius' Antrocom, 2010, Vol.6, No.1, pp.53-62, at p.55.

kept for the future crime cases as it is the case in Denmark or in Great Britain. On the other hand, the opposition argued that the collecting and keeping of DNA samples might transform the society from an innocent one into a society of convicts.

Another study which has privacy relevance in Mauritius was carried out in the context of e-governance. The project title is, 'Are Mauritians ready for e-Government Services?'[1528] This study found that Mauritians have low trust in terms of privacy, data protection, information security or cybercrime.[1529] According to the project researcher, the low rate of trust Mauritians have in ICT should consequently inspire policymakers to show their firm commitment to investigating e-justice and cyber-crime issues.[1530]

Somewhat related to the above is the fear particularly by politicians of interception of private communication (i.e. telephone tapping). This fear can well be demonstrated by the Mauritius parliamentary debates of 13 April 2004.[1531] During these debates, Dr. J.B David (member of Mauritius Parliament) asked the Prime Minister and Minister of Defence and Home Affairs whether he would state if telephone tapping was restored to in Mauritius. If that was the case, would he give the number of persons whose telephones had been tapped? Furthermore, he asked if such persons included politicians who were parliamentarians or non-parliamentarians, journalists and representatives of religion. In reply, the Prime Minister said telephone tapping was/is prohibited in Mauritius by virtue of section 46(o) of the Information and Communication Technologies Act 2001 unless authorised. The Prime Minister's reply attracted two more supplementary questions from Dr. David: had there been any request from any Ministry, or most likely from the Police and the Prime Minister's Office, for telephone tapping? To this question the Prime Minister replied, 'I have replied that when the Police wants to resort to telephone tapping in connection with criminal proceedings, whether pending or contemplated in Mauritius, they go to a judge sitting in Chambers.'[1532] The other question from Dr. David was: would the Prime Minister find out from the Commissioner of Police whether maybe without his knowledge

[1528] Shalini, R.T., 'Are Mauritians ready for e-Government Services?,' Government Information Quarterly, 2009, Vol.26, No.3, pp.536-539.
[1529] Ibid, p.537.
[1530] Ibid.
[1531] Mauritius National Assembly, Debate No. 5 of 2004, 'B/165 Telephone Tapping', Parliamentary Questions-Oral Answers, Tuesday 13th April, 2004, Mauritius National Assembly Website, http://www.gov.mu/portal/site/AssemblySite/template.MAXIMIZE/menuitem.6ee93699ee0e4d9c6179c38ea0208a0c/?javax.portlet.tpst=b00fa9180f29b8e9f534909e65c521ca_ws_MX&javax.portlet.prp_b00fa9180f29b8e9f534909e65c521ca_viewID=orans13apr04&javax.portlet.begCacheTok=token&javax.portlet.endCacheTok=token, last visited 22/03/2012.
[1532] Ibid.

telephone tapping was being resorted by the Police? The Prime Minister replied, 'I am giving the guarantee that this is not the case.'[1533]

A similar source of fears arises in the use of anonymity within the current sale of pre-paid SIM cards in Mauritius. These fears transpired in the course of parliamentary debates of 27 April 2004.[1534] During these debates Mr. M. Chumroo asked the Minister of Information Technology and Telecommunications whether there existed any control on the use of SMS. If that was the case, would he state the measures he had taken or proposed to take to ensure that there was no abusive use of such SMS? In his reply, the Minister noted that on average, not less than 40 million SMS messages were exchanged each month in Mauritius. He also noted that some individuals sent messages of an abusive language, indecent, obscene, menacing or otherwise objectionable nature. The Minister confirmed existence of reports about threat with rape and bodily violence and other forms of harassment arising from use of SMS. However he traced the root cause of all such abusive uses of mobile phones to reside in anonymity that people enjoyed from the system of sale of prepaid SIM cards. He noted that prepaid SIM cards were sold over the counter without any procedure for ascertaining the identity of the buyer. To eradicate the problem, the Minister suggested introducing mandatory registration of SIM cards in future.

A less obvious but relevant study was conducted in the context of use of public Internet kiosks in Mauritius.[1535] The study sought to investigate the determinants affecting individuals' intention and behaviour to use public Internet kiosks. One of the findings of this study is that subjective norm significantly affects individuals' intention to use ICT. This subjective normativity is attributable to the fact that Mauritius culture is largely collective. Partly this explains why the recently introduced E-Register System has not raised privacy concerns. The E-Register System is a system whereby alerts via automatically generated SMS are sent to responsible parties' mobile phones if their ward is absent or late at school.[1536] The system has been introduced in order to

---

[1533] Ibid.

[1534] Mauritius National Assembly, Debate No. 7 of 2004, 'B/229 Phones(Mobile)-SMS', Parliamentary Questions-Oral Answers, Tuesday 27th April, 2004, Mauritius National Assembly Website, http://www.gov.mu/portal/site/AssemblySite/template.MAXIMIZE/menuitem.6ee93699ee0e4d9c6179c38ea0208a0c/?javax.portlet.tpst=b00fa9180f29b8e9f534909e65c521ca_ws_MX&javax.portlet.prp_b00fa9180f29b8e9f534909e65c521ca_viewID=orans27apr04&javax.portlet.begCacheTok=token&javax.portlet.endCacheTok=token, last visited 22/03/2012.

[1535] Pee, L.G *et al.*, 'Bridging the Digital Divide: Use of Public Internet Kiosks in Mauritius', Journal of Global Information Management (JGIM), 2010, Vol.18, No.1, pp.15-38.

[1536] Speech of Honourable Tassarajen Pillay Chedumbrum, Minister of Information and Communication Technology, on Launching of E-Register at SSS Forest-Side, Boys Dept on 9th February 2011, http://www.gov.mu/portal/site/telcomit?content_id=8975860892a0e210VgnVCM1000000a04a8c0RCRD last visited 20/03/2012.

curb unjustified absenteeism of students in Mauritian public and private secondary schools which is becoming a major problem. According to the Mauritian Minister of Information and Communication Technology, the E-Register System provides also a database of all schools', students' and parents' details.[1537] Most of these details include personal information. Despite massive collection of personal information in computerised databases there have been no public concerns over privacy as a result of the introduction of the E-Register System. Yet cultural factors, particularly strong family ties have been sometimes regarded as having no or little influence in determining Mauritians' privacy concerns. At least in Mauritius such claims have been considered as 'out-dated concerns' as risks posed by modern technologies are no longer confined to a particular society.[1538] Nevertheless, there are still problems in absorbing the culture of data protection. This point is well explained by the Data Protection Commissioner for Mauritius:-

> 'However, the task is indeed an immense one to inculcate the culture of data protection into each citizen of this country. Let us not forget that even for those countries which have adopted data protection for 30 years, data protection was initially viewed as insignificant compared to other pressing agendas of the government the more so as it is quite a complex field and it is still a challenge for these countries to instil data protection principles in the routine of each citizen. Time has shown that such a concept is indeed the future guarantee for the individual today and tomorrow.'[1539]

The conclusion which can be drawn from the above analyses is that ICTs have played significant role to catalyse privacy concerns in Mauritius. However the pattern of its influence has yet been thoroughly examined. As it can be noted, sometimes there are clear privacy concerns as a result of individuals' interactions with ICTs in different contexts. At the same time such concerns in certain cases are lacking as it is the case with the E-Register System. Also significant to note, privacy is a relatively recent term in common use in Mauritius. It was firstly introduced vide the Bill of Rights in the Mauritian Independence Constitution in 1968.[1540] Moreover the attitudes of

---

[1537] Ibid.
[1538] Researcher's interview with Mrs. Drudeisha Madhub, Mauritian Data Protection Commissioner, on 4/07/ 2011 in Port Louis, Mauritius.
[1539] Madhub, D., 'Data Protection from an Employment Perspective', Paper Presentation to Groupe Mon Loisir Ltd, 5th July 2011, Mauritius Data Protection Office's Website, http://www.gov.mu/portal/site/dataprotection/menuitem.079dc52bbf696f8858c64510a0208a0c/ last visited 21/03/2012.
[1540] The Constitution of Mauritius, 1968, Arts 3(c) and 9.

privacy by Mauritians are largely affected by lack of culture of data protection rather than the Mauritian society's culture. However the latter may still have impact upon the former and vice versa.

5.4 Legal and Regulatory Framework

The legal and regulatory framework for privacy and data protection comprises of two major legal sources: the Constitution and legislation. The legislative source can be further divided into two groups. These are the omnibus data protection legislation and sectoral legislation addressing data privacy issues. There are also subsidiary legislation, codes of practice and guidelines developed under the general data protection legislation. Apart from sectoral legislation there exist a number of pieces of legislation which have *ad hoc* provisions relevant to data privacy protection. However there is no known case law decided by Mauritian courts which directly address data privacy complaints. As a result, case law is an insignificant source. Yet since its establishment to date, the Mauritian Data Protection Commissioner (DPC) has rendered down 7 decisions arising from different complaints filed to her.

As alluded to, the discussions and analyses in this chapter are limited to mainly the general data protection legislation. The other sources are minimally analysed. Such analysis is important to show how the general data privacy legislation is related to the specific ones. Also significant, the analysis will indicate which legislation was repealed and which one was maintained by the general data privacy legislation.

5.4.1 The Constitution of Mauritius 1968

The Mauritian Constitution explicitly recognises privacy as a basic fundamental human right. Art 3(c) states:-

> 'It is hereby recognised and declared that in Mauritius there have existed and shall continue to exist without discrimination by reason of race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, each and all of the following human rights and fundamental freedoms –
> (a)...
> (b)...and;

(c) the right of the individual to protection for the privacy of his home and other property and from deprivation of property without compensation'.

Art 3(c) is further expanded and consolidated in Art 9 of the Mauritian Constitution. The latter states that 'except with his own consent, no person shall be subjected to the search of his own person or his property or the entry by others on his premises.'

In contrast to the corresponding provisions in the Universal Declaration of Human Rights 1948 and the International Covenant on Civil and Political Rights 1966 to which Mauritius is bound, Arts 3 (c) and 9 of the Mauritian Constitution are narrowly formulated. While in the former privacy is guaranteed in the contexts of family, home, correspondence, honour and reputation in the latter it is only confined to home and other property. Although there is currently no known case law by Mauritian courts interpreting Arts 3(c) and 9 of the Constitution, it can be argued that the latter have the potential of embracing the other elements in the UDHR and ICCPR. This view is strengthened by the fact that in some jurisdictions like the United States where the constitution does not expressly guarantee protection of privacy, the U.S Supreme Court has concluded that such a right exists.[1541] Indeed, the disclosure of personal information, which is nowhere stated in the U.S Constitution, can still be secured under certain circumstances.[1542] Hence the whole issue depends on courts' interpretation.

However the value of Arts 3(c) and 9 of the Mauritian Constitution can be appreciated from the fact that they are embedded in the constitution. The latter is the superior source of law in Mauritius. This means that any law or its provisions including the data privacy legislation must pass the standard set by the constitution for its validity. It can be submitted that despite their shortcomings, Arts 3(c) and 9 of the Mauritian Constitution are the legal source for the existence of the Data Protection Act 2004 and other legislation relevant to data privacy protection.

Apart from being a legal source for the Data Protection Act 2004, the Constitution of Mauritius makes it clear that it applies without discrimination of place of origin. This means that citizens and non-citizens of Mauritius can seek constitutional protection once their right to privacy is

[1541] See e.g. Hammitt, H., 'A Constitutional Right of Informational Privacy', Government Technology, 1998, http://www.govtech.com/magazines/gt/A-Constitutional-Right-of-Informational-Privacy.html last visited 21/03/2012; see also the Opinion of the Supreme Court of the United States in National Aeronatics and Space Administration *et al*, v. Nelson *et al*, where the Supreme Court avoided the use of the right of informational privacy, http://www.supremecourt.gov/opinions/10pdf/09-530.pdf last visited 21/03/2012.
[1542] Ibid.

infringed. Concomitantly, any restriction of application of the right to privacy in any legislation on the basis of place of origin may be regarded as invalid.

The right to privacy in Arts 3(c) and 9 of the Mauritian Constitution is however not absolute. It is subject to certain limitations as designed to ensure the enjoyment of such right by any individual does not prejudice the rights and freedoms of others or the public interests.[1543] These set of limitations are specifically stipulated in Art 9(2) which include an expansive list. The limitations include those relating to the interests of defence, public safety, public order, public morality, public health, town and country planning, the development or utilisation of property of any kind in order to promote public benefit; for purposes of protecting the rights and freedoms of other persons; tax purposes; and enforcement of judgement or order of the court in any civil proceedings. Yet the general derogations are provided in Art 18 of the Mauritian Constitution. It is submitted that while the exercise of the right to privacy needs to be balanced with other rights, it is doubtful if the expansive list of derogations laid down in the constitution may leave privacy right as having any practical relevance.

5.4.2 The Data Protection Act 2004

The Data Protection Act 2004(DPA) is the principal data privacy legislation in Mauritius. The Act was passed by the Mauritian Parliament on 1 June 2004. It was immediately assented to by Sir Enerood Jugnauth, the President of Mauritius on 17 June 2004. However the Data Protection Act was proclaimed in three phases. The first proclamation concerned the following sections 1; 2; 4; 5(b),(c),(e),(g),(h),(i),(j); and 6. These provisions were brought into force on 27 December 2004 through Proclamation No. 45 of 2004.[1544] It is important to mention that these sections relate to the short title of the Act, interpretation, establishment of the office of DPC and vesting it with limited functions, confidentiality and oath of the Commissioner and other DPC's staff respectively. Through Proclamation No.45 of 2004 Mauritius became the earliest African country to establish the office of Data Protection Commission and make it operational. This means that the office of DPC in Mauritius preceded even Cape Verde and Seychelles which adopted data protection legislation much earlier. It also preceded Tunisia's *Instance Nationale pour la Protection des Données à Caractère Personel* (INPDCP or Data Protection Authority). Tunisia's data protection legislation was adopted one month after Mauritius'. As alluded to, this was one of the reasons for handpicking Mauritius as the case of the present research.

[1543] The Constitution of Mauritius 1968, Arts 3.
[1544] Proclamation No. 45 of 2004 was signed by the Mauritian President on 15th December 2004.

The second set of proclamation was made through Proclamation No. 5 of 2009.[1545] The latter brought the rest of the provisions of the Data Protection Act 2004 in full operation as from 16 February 2009. However the proclamation left unproclaimed section 17 of the DPA which deals with the DPC's powers of entry and search. Accordingly, the powers of entry and search were not exercisable by the DPC at that time. It is imperative to note that the piecemeal proclamation of the Data Protection Act 2004 was adopted in order to establish the office of DPC and provide opportunity for the Commissioner to develop the necessary guidelines and codes of practice under section 5(b) and preparations of regulations by the Prime Minister.[1546] Both of them were/are necessary to operationalise the principle legislation. As important as it was, the piecemeal proclamation had its shortcomings. First, the first proclamation overlooked to bring into force sections 56 and 65. Section 56 incorporates detailed provisions on the Commissioner's functions to issue or approve codes of practice or guidelines. In this way section 56 is an elaborative provision of section 5(b) of the Data Protection Act which was proclaimed on 27 December 2004. As for section 65, it empowers the Prime Minister to make regulations to operationalise the Act. In the exercise of these powers, the Prime Minister may consult the Data Protection Commissioner. Some legal and practical problems which arise here are that the Data Protection Commissioner and Prime Minster invoked the application of sections 56 and 65 well before they were proclaimed.[1547] This supports the argument that the two provisions had to be proclaimed with the other provisions in the first proclamation. Yet this could not result into serious legal uncertainties because the guidelines and regulations became applicable only after the second proclamation of the rest of provisions of the DPA. To be sure, the Data Protection Regulations 2009 were made by the Prime Minister under section 65 of DPA on 3 March 2009 after consultation with the Commissioner.[1548] However they were brought into force on 16 February 2009.[1549] The latter was the date the second proclamation was made.

Another legal and practical point is that under sections 5(b) and 56, the DPC has the mandate to issue guidelines or codes of practice or approve either of them. Based on these provisions the guidelines prepared by the Commissioner in 2007 could have become operational even in the

[1545] Proclamation No. 5 of 2009 was signed by the Mauritian President on 4th February 2009.
[1546] In her presentation 'An Overview of the Mauritian Data Protection Act' dated 30 November 2007 Mrs. Drudeisha Madhub, the Mauritian Data Protection Commissioner mentioned that the instrument of proclamation together with the required regulations and relevant guidelines had already been sent to the Senior Chief Executive of the Prime Minister's Office, see Mauritius Data Protection Office's Website,
http://www.gov.mu/portal/site/dataprotection/menuitem.079dc52bbf696f8858c64510a0208a0c/
last visited 21/03/2012.
[1547] Ibid.
[1548] Data Protection Regulations 2009, Government Notice (G.N) No. 22 of 2009.
[1549] Ibid, R.8.

absence of the regulations. But this would practically be impossible. First, the Commissioner's guidelines touched upon most of the provisions of the Data Protection Act 2004 which were yet to be proclaimed. Second, such guidelines depended upon the existence of the regulations as the other source of enabling provisions. These legal and practical hurdles partly offer explanation why it took more than four years for the Data Protection Act to come into full operation since it was passed in 2004.

So far the DPA has been amended twice. The first amendment was passed on 15 April 2009 through section 2 of the Additional Stimulus Package (Miscellaneous Provisions) Act 2009.[1550] This provision, among others, amended section 17 of the Data Protection Act 2004 on Commissioner's powers of entry and search. The same section repealed the contentious section 21 of the Data Protection Act 2004 on the Prime Minister's powers to give the Data Protection Commissioner direction in the discharge of her duties. The Stimulus Package Act was assented on 16 April 2009 and proclaimed on 22 May 2009 through Proclamation No. 11 of 2009. Accordingly section 17 of the DPA is currently in force making the third and final phase of proclamation of the Act. The second amendment was passed on 22 July 2009 through section 10 of the Finance (Miscellaneous Provisions) Act 2009. This Act was assented on 30 July 2009. However, while section 49 of the Finance Miscellaneous Act declared different commencement dates for various provisions, it did not do so with respect to section 10 which amends various provisions of the Data Protection Act 2004. It is important to note that although the Finance Miscellaneous Act was published on the DPC's Website as a source of data protection legislation there is yet a commencement date published by the Commissioner.

The Data Protection Act's amendments were necessitated by various reasons. The National ICT Policy clearly states that it was to meet the need for Mauritius to be potentially recognised by the European Union as a third country with an adequate level of protection.[1551] The Data Protection Commissioner has specifically explained the reasons behind the Act's amendments through the Stimulus Package Act in two aspects: to enhance prospective registration of data processors and also to give more independence to the Commissioner in the exercise of her function under the DPA.[1552] Yet, in her First Annual Report(February 2009-February 2010), the Commissioner

[1550] Additional Stimulus Package (Miscellaneous Provisions) Act 2009, Act No. 1 of 2009.
[1551] See, e.g. Mauritius National ICT Policy 2007-2011, pp.1-18, at pp.7-8; Gayrel, p.20, note 1334, supra.
[1552] Madhub, D., 'Data Protection Implications for Our DNA Bill', Paper presented by the Commissioner on the 9th June 2009 at the Awareness Workshop on Legal Aspects of the Use of Human DNA, Mauritius Data Protection Office's Website,
http://www.gov.mu/portal/site/dataprotection/menuitem.079dc52bbf696f8858c64510a0208a0c/

assigns a different reason: 'the Commissioner was required to amend and update the Data Protection Act to secure better chances of accreditation with the European Union for Mauritius to be recognised as an adequate country in data protection to facilitate the transfers of personal data from the European Union to Mauritius and thus attract more investment in mainly the ITES/BPO(i.e. Information Technology Enabled Service/Business Process Outsourcing) sectors of the Mauritian economy.'[1553] Admittedly, both reasons advanced by the Commissioner are broadly in line with the policy statement in the Mauritian National ICT Policy.[1554] This is because the need for independent data protection authority as previously stated by the DPC is central to the functioning of data privacy legislation under the European Directive 95/46/EC.

5.4.2.1 Need for Data Protection Legislation

There are two major reasons in the discourse of data privacy in Mauritius why the Island adopted omnibus data protection legislation. The first is the protection of individuals' right of privacy as a result of potential risks posed by use of ICTs. The second reason is the attraction of foreign investments in Mauritius. This is also commonly known as economic justification theory or imperative. It is necessary to investigate the relative strength of each of these reasons in the adoption of the Data Protection Act 2004. The rationale for this investigation is twofold: it determines the legislative process and competing interests involved and consequently practice and enforcement of the legislation.

However in attempting to find out the relative position of the above reasons in adopting the data privacy legislation statutory and non-statutory aids to interpretation are used. The former include intrinsic (text based) and non-intrinsic (non-text based). The non-statutory aids to interpretation are used here as they provide the broader context in which the data privacy legislation developed.

The Explanatory Memorandum to the Data Protection Bill (No. XV of 2004) reads as follows:-

> 'The object of this Bill is to provide for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, manipulate, record or store data relating to individuals.'

---

last visited 21/03/2012.

[1553] Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010, p.4.

[1554] Mauritius National ICT Policy 2007-2011, pp.1-18, at pp.7-8.

The above object clause is reproduced as the long title of the Bill itself and finally the Data Protection Act 2004, after the former was passed into law. Apart from the object clause and the long title of the Data Protection Bill and Act which are silent on economic agenda behind the DPA, there is similarly nowhere in the Bill or Act any mention of economic justification as an object served by the Data Protection Act 2004. Superficially, it sounds as if the DPA was adopted to serve a single object: protection of individuals' right of privacy. Moreover, the fact that the protection of privacy expressly manifests itself in the long title of the DPA suggests that it is the dominant reason why the data protection legislation in Mauritius was adopted. Yet the *Hansard* (the printed transcripts of parliamentary debates) of the Parliament of Mauritius of 1 June 2004 speaks the opposite. While the *Hansard* repeats privacy protection as the reason for adopting the DPA, it frequently and dominantly mentions ITES/BPO as the primary agenda served by the Data Protection Act 2004. In the beginning of his address, while moving the Data Protection Bill to be read for the second time, the Prime Minister spent a considerable time and space to trace the development of the ICT sector since 2000 as the fifth pillar of the Mauritian economy.[1555] After lying that foundation, the Prime Minister said, 'in order to build and maintain confidence that Mauritius is a reliable and sure destination for ICT business, we also have to ensure that we have the proper legal framework.'[1556] Interestingly, until that stage the Prime Minister made no mention of protection of privacy as a fundamental right. Although subsequently, he clearly recapitulated the object of the Data Protection Bill as nearly as in the Explanatory Memorandum, 'the Bill in front of us is about protection of the fundamental privacy rights of individuals, and all data controllers who are established in Mauritius or use equipment in Mauritius for processing data will need to comply with this law',[1557] he emphatically repeated the economic justification theory as behind the adoption of the data privacy legislation: 'it will also constitute a strong incentive for prospective overseas agencies to do business in Mauritius in the ICT sector proper, or in businesses where personal data is used routinely'.[1558] To further demonstrating the priority of business agenda the Prime Minister went on: 'the European Union (EU) countries are strictly regulated by the EU Directives and hesitate to do business with countries which do not have the same or similar legal protections for the privacy rights of individuals'.[1559]

[1555] Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004), pp.77-78.
[1556] Ibid, p.78.
[1557] Ibid.
[1558] Ibid.
[1559] Ibid.

The business agenda is also amplified by Mr. D. Jeeha, the Minister of Information Technology and Telecommunications. In his speech, Mr. Jeeha said, 'the primary objective of the passing of the Data Protection Bill is to protect individuals with regard to the processing of personal data and on the movement of such data.'[1560] However he capitalised that, 'this Bill comes at the right moment with the start of activities by internationally renowned companies in the field of business process outsourcing at the Ebene Cybercity.'[1561] The Minister made several repetitions demonstrating the link between the adoption of the DPA and promoting business interests. For example, Mr. Jeeha pointed out, 'this Bill will additionally provide the necessary comfort to investors in the IT Enabled Services and Business Process Outsourcing sectors.'[1562] He pointed also, 'the Data Protection legislation will help to create appropriate confidence among investors and foreign companies to the effect that the data they send to Mauritius for back-office operations is indeed safe and that appropriate statutory mechanisms in place should a breach of data take place.'[1563]

Beyond parliamentary debates, the reasons for adoption of the DPA in Mauritius appear in the National ICT Policy 2007-2011. The latter sets out ICT sector as the fifth pillar of the economy of Mauritius. One of the objectives of the Policy in supporting its broad vision is to develop the export markets for ICT services and BPO/ITES. This entails, among other policy priorities, to strengthen the legal and regulatory framework. In this context, the National ICT Policy clearly sets an agenda for amending the Data Protection Act 2004 to support the Policy's vision and objectives.[1564] The protection of individuals' privacy is insufficiently covered in the ICT Policy relatively to the business interests.

Another source where the reasons behind the adoption of the DPA can be traced is the various presentations of the Data Protection Commissioner. The accounts given in such presentations are not consistent. Sometimes privacy appears as the sole reason for adoption of the DPA. Yet in certain cases this is business outsourcing industry. And, in some occasions both reasons are given to support the existence of the DPA. However these reasons are similarly inconsistent in their weight. For instance, in her presentation[1565] of 30 November 2007 the Commissioner

[1560] Ibid, p.96.
[1561] Ibid.
[1562] Ibid.
[1563] Ibid.
[1564] Mauritius National ICT Policy 2007-2011, p.7.
[1565] Madhub, note 1546, supra.

restated the object of the DPA by adopting the long title of the Act. She took investment as the second priority of the law. Yet in her presentation of 5 October 2011 the Commissioner seems to put more emphasis on investment than privacy. In that presentation the slide presentation asked, 'why have a DPO in Mauritius?' Her reply was as follows:-

> 'The need was felt when investment in the ITES/BPO sector was being prejudiced due to lack of an appropriate legal data protection framework in Mauritius. However, since data protection is essentially a human right issue as it concerns the protection of the personal data of living individual, the scope of data protection is not restricted to purely economical considerations or gains but also encompasses the broader perspective of the right to privacy or the right to be left alone of every citizen of this country.'[1566]

However, during interview with the researcher of this thesis on 4 July 2011 in her office (Port Louis, Mauritius), the Commissioner made clear to the question: 'why did Mauritius adopt data protection legislation' that protection of privacy of an individual was a priority consideration. She noted that privacy in Mauritius is protected in the constitution. However, the constitutional protection is very broad to protect infringement of privacy resulting from ICTs. This became the reason for adopting the data protection legislation which though limited it creates a specific legal framework for processing personal data. The Commissioner clearly pointed that economic or business process outsourcing was secondary and incidental to the privacy of the individuals in Mauritius.

The statement of Mr. Raju Jaddoo, the Managing Director of the Mauritius Board of Investment and board member of the COMESA Regional Investment Agency is clearer on the business agenda behind the adoption of DPA. He posits:-

> 'Since 2004, the island's IT-enabled and BPO service sectors have witnessed an average growth rate of 30-35%, generating wide-scale social and economic benefits for the country. This growth has been accompanied with the consolidation of business processes and the whole sector is demonstrating a

[1566] Madhub, D., 'The Data Protection Office in Mauritius-The Challenges Ahead', Paper presented by the Commissioner on 5 October 2011 to the ICT-BPO Community, see Mauritius Data Protection Office's Website, http://www.gov.mu/portal/site/dataprotection/menuitem.079dc52bbf696f8858c64510a0208a0c/ last visited 23/03/2012.

> strong growth potential....The legal framework governing ICT has been developed in accordance with international norms and best practices. A Copyright Act, a Cybercrime and Computer Misuse Act and Electronic Transaction Act are currently in force. These, along with the recent promulgation of the Data Protection Act, illustrate the government's commitment to enhancing the credibility of the Mauritian outsourcing industry.'[1567]

The above analyses clearly demonstrate that despite the object clause of the Data Protection Bill and the long title of the Data Protection Act 2004, both protection of individuals' privacy and securing foreign investment were the reasons for the adoption of the DPA. However in relative terms, the latter played a significant role as against the former in the adoption of DPA. Yet in interpretation of the DPA the two objectives must be balanced. This is because over protection of privacy may impede free flow of information resulting into distortion of business process outsourcing which is the fifth pillar of economy in Mauritius. At the same time, over protecting business may result into violation of individuals' privacy. Therefore only a fair balance between the two objects may effectively result into smooth implementation of the DPA.

5.4.2.2 Legislative Process

The Data Protection Bill 2004 was introduced in the Mauritian Parliament on 25 May 2004 and passed into law on 1 June 2004. The first reading of the Bill was on 25 May 2004 while the second and third readings were on 1 June 2004. According to Rules 52 and 53 of the Mauritius Standing Orders and Rules of the National Assembly 1995 (i.e. Parliamentary Rules), only the short title of a Bill is read and no debate is allowed in the first and third readings. However under Rule 56, that is, during the second reading-the long title of the Bill is read. Moreover debates covering the principles and general merits of the Bill are permitted. During the second reading amendments, omission or addition of all or some words can be made but not in any other stage. Accordingly, the Data Protection Bill 2004 was debated in hours and passed as law on the same date, i.e. 1 June 2004.

[1567] Jaddoo, R., 'Mauritius Board of Investment: Mauritius-The Island of Opportunity', http://www.the-chiefexecutive.com/projects/island-of-mauritius/ last visited 23/03/2012.

However before the Bill was introduced in the National Assembly, it was not or at least it was subjected to limited consultation process. The latter did not involve at all members of the public. The Parliamentary *Hansard* reveals this shortcoming through Dr. A. Boolell:-

> 'Mr. Deputy Speaker, Sir, we, of course, welcome the Bill, but we intend to sound a note of caution. And with the breakthrough in ICT and easy accessibility to computer usage and Internet, we can say that the legislation is timely. But, however, let us call a spade a spade. Enforcement, Mr. Deputy Speaker, Sir, may be difficult because the Internet is the property of everyone and no one. I am sure you will agree, Mr. Deputy Speaker, Sir, that this is a complex Bill. This legislation, in our opinion, should have been circulated to invite participation from all relevant stake players. Unfortunately, the Bill has not been widely disseminated, but we agree that the Data Protection Bill, in almost every country, is almost a copycat of each other and available on the net....It would have been better if the Bill could have been widely circulated, if it could have had vital input from all the stake players and if a copy of the Bill could have been sent to the National Economic and Social Council so that input could be obtained. Elsewhere, Mr. Deputy Speaker, Sir, there has been a While Paper, the matter has been widely discussed because we are talking of a balancing Act and we have to make sure that there is no infringement upon privacy and that human rights issues are strictly adhered to.'[1568]

Somewhat similar to the above observation, Mr. M. Dowarkasing submitted, 'I would like to say this Bill is a very complex one and we should proceed in phases to make the law known to all stakeholders, especially the data controllers and the public. Since this Bill is sensitive as it deals with the personal privacy, great care has to be taken to strike the right balance between technological advance and privacy.'[1569]

Further evidence in support of the view that the Data Protection Bill 2004 was not put into public consultation is given by Dr.N.Ramgoolam, the leader of the opposition in the Mauritius Parliament. Dr. Ramgoolam observed, 'I know that hon. Dr. Boolell and hon.Dowarkasing have said it. It is an important and complex Bill which deals with the privacy rights, from what I have

[1568] Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004), pp.85-86, 90.
[1569] Ibid, p.103.

heard the Bill has not been debated enough outside in the public and people are not aware of what are the dangers, perhaps they could have been given more time.'[1570] Interestingly, in his reply to the call for public consultation, the Prime Minister said, 'we can always at any point in time, improve and plug loopholes.'[1571] Based on this opinion he assured the members of Parliament that the Bill, once voted, the Act would be referred to the National Economic and Social Council, to the Human Rights Commission, and to anybody, who would have time to look at the Act that had already been voted and propose amendments and improvements to the piece of legislation.[1572]

It is imperative to point that the legislative process of the Data Protection Act 2004 did not as well involve the Mauritius Law Reform Commission. There were obvious reasons for this. First, although the Law Reform Commission was established since 1992[1573] by 2004 when the Data Protection Bill 2004 was being considered it had no any staff except its Chairperson.[1574] Moreover it had no library.[1575] Second, the limited projects it could handle did not include the DPA.[1576] Since the Law Reform Commission was the body to carry out public consultations, its non- involvement increased constraints to the legislative process.

The overall implications for the legislative process leading to the adoption of the DPA leave a lot to be desired. It has partly made difficult to win compliance from both the data controllers and subjects. This is because majority of persons, the subjects of the operation of the DPA, are ignorant of the existence and/or application of the provisions of the Data Protection Act. In the First Annual Report, the Commissioner points out lack of awareness of the DPA as one of the most challenging areas of enforcement.[1577] Despite that fact the Commissioner maintains that ignorance of the obligations under the DPA is not a legitimate excuse, especially given the fact that data protection obligations are more often simply just a question of adopting good civilian manners.[1578] Arguably, 'adopting good civilian manners' particularly in the complex context of data privacy needs one to appreciate the privacy risks, policies and regulatory frameworks in

[1570] Ibid, p.104.
[1571] Ibid, p.109.
[1572] Ibid.
[1573] Mauritius Law Reform Commission Act 1992, (Act No.33 of 1992), proclaimed on 1st December 1992 through Proclamation No. 2 of 1993.
[1574] Mauritius Law Reform Commission Annual Report June 2004, pp.1-9, at p. 4.
[1575] Ibid.
[1576] Ibid, pp.5-7.
[1577] Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010, p.42.
[1578] Ibid, p.6.

place. That is why for example, unlike other ordinary statutes and especially penal laws which states 'ignorance of law' is no defence, data privacy legislation incorporates provisions requiring the Commissioner to educate the public. To be sure section 5(g) of the Data Protection Act 2004 states that the function of the Commissioner shall be to take such measures as may be necessary so as to bring to the knowledge of the general public the provisions of this Act.

It can also be argued that the above legislative process partly explains why Mauritius adopted the DPA. The Act was adopted as a matter of urgency suggesting that it aimed to instil confidence to foreign investors. As alluded to, the Act had to be voted in the first place and then be subjected to some sort of consultation afterwards. Moreover, the amendments which have so far been made to the DPA were/are intended to meet compliance to the 'adequacy' standard in Directive 95/46/EC (see 5.4.3). More amendments are expected as Mauritius is currently seeking from the European Union accreditation of its DPA (see 5.4.3).

5.4.2.3 Scope and Application

Section 3 of the Data Protection Act provides that the Act shall bind the State. Literally this means that the DPA applies to public bodies only. The definition of 'data controller' in section 2 does not either suggest if the DPA applies to private bodies. This is somewhat contrary to the corresponding definition of 'data controller' in the European Directive which defines a 'data controller' in terms of public or private status. Nonetheless, when reading section 54 it becomes certain that the DPA applies to private bodies and individuals as well. This provision excludes the application of the Act when data processing takes place purely in the context of family, household affairs or for recreational purposes. This exemption suggests that in any other cases where individuals process personal data, the Act binds them. Also significant to note the *Hansard* indicates that the DPA has a wide application in that it binds not only the State, but also a data controller.[1579] While it may sound as if a 'data controller' is an individual or private entity, the notion of 'controller' includes the State and its agencies. The Data Protection Commissioner has similarly made this point clear in most of her presentations that the DPA applies to both public and private bodies and individuals.[1580]

[1579] Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004), p.84.

[1580] See e.g., Madhub, D., 'An overview of the Data Protection Act and its implications as regards registration and data subject access requests for the Ministry of Information and Communication Technology', Paper presented by the Commissioner on the 10th June 2009 at the Ministry of the Information and Communication Technology, see Mauritius Data Protection Office's Website,

Moreover the DPA applies to both automatic and manual processing of personal data.[1581] Yet such processing of personal data is limited to individual natural/physical persons only called the 'data subject'.[1582] Legal/juristic persons are outside the purview of the Act.

Territorially, the DPA has a broad scope. It applies to a data controller who is established in Mauritius.[1583] In addition such a controller must process personal data in the context of that establishment.[1584] However in case a controller is not established in Mauritius but uses equipment in Mauritius for processing data such a controller is subject to the application of the DPA.[1585] In that case he or she has an obligation to nominate a representative who resides in Mauritius to carry out his or her data processing activities through an office in Mauritius.[1586] But if such controller uses such equipment for the purpose of transit through Mauritius, the Act does not apply upon him/her.[1587]

As relating to non-application, the DPA contains an extensive exemption regime in Part VII (ss 45-54). The exemption is either partially or wholly. The list of matters exempted are national security(s 45); crime and taxation(s 46); health and social work(s 47); regulatory activities(s 48); journalism, literature and art(s 49); research, history and statistics(s 50); information available to the public under an enactment(s 51); disclosure required by law or in connection with legal proceedings(s 52); legal professional privilege(s 53); and domestic purposes(s 54). Partial exemption usually takes the form of relieving the controller from obligation of notification and application of certain data protection principles. With the exclusion of 'health and social work' Gayrel does not seem to worry about the Mauritian data exemption regime in the DPA.[1588] She contends that the rest of the exemptions can be justified and do not raise many issues.[1589] However she is concerned with two things. First, although these exemptions are only allowed 'to

---

http://www.gov.mu/portal/site/dataprotection/menuitem.079dc52bbf696f8858c64510a0208a0c/
last visited 24/03/2012. In this presentation the Commissioner said, 'if you, as an individual or an organisation, collect, store or process any data about living people on any type of computer or in a structured filing system, then you are a data controller'. See also, Madhub, note 1565, supra, where the Commissioner clearly points out, 'a data controller is any private or public entity controlling the processing of personal information.'

[1581] 'Processing' means any operation or set of operations which is performed on the data wholly or partly by automatic means, or otherwise than by automatic means, Data Protection Act 2004, s.2.

[1582] 'Data subject' means a living individual who is the subject of personal data, Data Protection Act 2004, s.2.

[1583] Data Protection Act 2004, s.3 (3), (a).

[1584] Ibid.

[1585] Ibid, s.3(3),(b).

[1586] Ibid, s.3 (4).

[1587] Ibid, s.3(3),(b).

[1588] Gayrel, p.21, note 1334, supra.

[1589] Ibid.

the extent that such an application would be likely to prejudice' they are questionable, particularly because of the wide range of regulatory activities.[1590] Arguably, this is one of the things Gayrel should have worried about in the first place. Second, 'crimes and taxation' matters (s 46), notably the processing of personal data 'for the prevention and detection of crime' and 'apprehension or prosecution of offenders' are exempted from various principles of the Act, but surprisingly are not exempted from the obligation of information imposed on controllers according to section 22 of the Act.[1591] She holds that that may be an unintended loophole of the Act; otherwise the Mauritian police would have to inform suspected people about fraudulent activities under investigation.[1592] In Gayrel's opinion, this omission nevertheless raises the issue as to whether exemptions to data protection principles for police activities have been duly assessed.[1593] Gayrel's doubts have to be explained in the entire legislative process of the DPA (see 5.4.2.2).

Taking the entirety of the Mauritian context as already considered, the exemption regime leaves a lot to be desired. This is clearly captured in the *Hansard*. During the Mauritian parliamentary debates of the Data Protection Bill 2004, the exemption regime was one of the issues which attracted heated debates. For parliamentarians it was argued that the exemption regime contained a too long list virtually leaving nothing to be protected or regulated.[1594] They also argued that it would be difficult to justify certain exemptions.[1595] Two illustrations cited by the parliamentarians need mention. In exempting controllers with respect to physical and mental health from granting data subject's access; the argument is that health data are generally of confidential nature and cannot be disclosed without the consent of the individual concerned, i.e. the patient.[1596] Hence a patient cannot be blocked access to his or her own medical information. Moreover, a data controller can not disclose such information to third parties without the patient's consent. The only acceptable exemptions, according to parliamentarians, can be limited to circumstances where either there is a statutory requirement to disclose, court order or public interest justification, such as significant risks to others.[1597] The second illustration concerns data retention by the police. The submission by the leader of the opposition during debates is appealing. It deserves a direct quote:-

---

[1590] Ibid.
[1591] Ibid.
[1592] Ibid.
[1593] Ibid.
[1594] Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004), p.101.
[1595] Ibid.
[1596] Ibid.
[1597] Ibid.

> 'Then there are usual blanket covers given to national security, but the Prime Minister knows that we need to have strong safeguards as there is a great deal of information which is secret and which has nothing to do with security matters. I hope the Prime Minister knows what I am saying because there is a lot of information coming to you which is meant to be secret and which has nothing to do with the security of State. This is something we need to make sure that we have safeguards because the Police can put a lot of data on the central computer, they can put the records, for example, all criminal convictions, etc., but how long are they going to stay there?'[1598]

The government's counter arguments to the members of parliament are that the exemptions are not provided against keeping of data in any database as these concerned only with notification and few principles only.[1599] Moreover, the Prime Minister categorically said, 'I cannot agree with hon. Dowarkasing that the list of exemptions is so long that there is nothing left to protect. No, that is not the case; the list of exemptions is restrictive and there would be plenty of scope left for protection of personal data.'[1600] It can be submitted that once a set of activities are excluded from the application of the DPA, information about individuals can be processed without any compliance to the Act. Moreover, based on the parliamentary debates surrounding the DPA's exemption regime, it is difficult to see how the exemptions, with whatever good justification, cannot be abused. This view is further strengthened by lack of proper safeguards surrounding the exemption regime. Section 45 of DPA on national security serves as an illustration. Under this provision, the Prime Minister can certify a particular case as one falling under section 45 hence exempted from the application of DPA. The powers given to the Prime Minister are important to the security of the state but are susceptible to abuse as no safeguards are provided. This point will further be discussed in part 5.4.2.5.

5.4.2.4 Data Protection Principles

The basic principles of data processing in the Data Protection Act 2004 are provided in the First Schedule titled 'Data Protection Principles'. This schedule contains eight principles closely patterned to the European Directive 95/46/EC. However some authorities have maintained that

[1598] Ibid, p.105.
[1599] Ibid, p.91.
[1600] Ibid, p.110.

the DPA draws its inspiration from both the European Directive and the *OECD Guidelines* as opposed to national laws of EU member states or other countries beyond Europe.[1601] Be as it may, in contrast to these two instruments, the eight principles in the DPA are framed without sufficient details. During parliamentary debates on the Data Protection Bill 2004, this issue was raised. However, the government made plainly that in the Mauritian legislation only the eight principles have been mentioned and it has been left to the Commissioner, at his discretion, to come up with codes of practice.[1602] This approach may pose two difficulties. First, as the field of data privacy is new in Mauritius, development of such codes of practice creates great challenges to formulate. The Commissioner may end up lifting codes of practice elsewhere in Europe and approve them. Second, the concept of 'discretion' may absolutely leave the Commissioner free from any obligation to consult anybody, be it stake players or experts. This may be dangerous particularly during the implementation stage of the Act. Yet in the exercise of such powers, the Commissioner has developed various codes of practice and guidelines. The latter provide some insights in the understanding and interpretation of the eight principles. Two of these codes directly apply here: 'A Practical Guide for Data Controllers & Data Processors -Volume 1' [1603](i.e. Practical Guide) and 'Data Protection-Your Rights -Volume 3'[1604] (i.e. Your Rights). Both of them are considered in the course of discussing the data protection principles enshrined in the First Schedule of the DPA.

The 'First principle' states that personal data shall be processed fairly and lawfully. The criterion of 'fairness' is extensively covered in Rule 1 of the Practical Guide. Under this Rule 'fairness' is understood in terms of collection hence 'fair collection' and processing hence 'fair processing'. As for 'fair collection' this is meant to make the data subject fully aware of the fact that his or her data is being collected. This entails provision of identity of the controller or processor; specifying the purpose of the collection; identifying persons to whom data will be disclosed; specifying whether supply of information is voluntary or obligatory; informing about the consequences for the individual if the required information is not provided; specifying whether or not consent of the individual is required for any processing of the information; and informing the right of access of the individual and the possibility of correction or destruction of personal data to be provided

[1601] See e.g. Gayrel, p.20, note 1334, supra.
[1602] Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004), Ibid, p.91.
[1603] Mauritius Data Protection Office, 'A Practical Guide for Data Controllers & Data Processors-Volume 1', http://www.gov.mu/portal/goc/dpo/files/Guidvol1v3.pdf last visited 25/03/2012.
[1604] Mauritius Data Protection Office, 'Data Protection-Your Rights -Volume 3', http://www.gov.mu/portal/goc/dpo/files/Guidvol3v3.pdf last visited 25/03/2012.

by him or her. Most of these details are provided as part of controller's obligations in section 22 of the DPA.

However, the above details are not required to be provided in two scenarios. First, is in case of secondary or future uses of the personal data under section 22(3)(a) of the DPA if there is repetition of the same information without any material differences. Yet this exemption applies only in limited period of 12 months since the previous collection. In any other case other than those exempted, the controller must give the above information afresh. Second, is where under section 22(3)(b) of the DPA, the data subject cannot reasonably expect to be identified from the personal data collected.

Section 22(2) of the DPA requires the controller to give certain information to the data subject at the time of collection of data identifying him or her, stating the purpose of collection, etc. Rule 1 of the Practical Guide requires that where it is practically impossible to give such information prior to collection, the controller must provide it as soon as possible after collection.

On the other hand, 'fair processing' is understood in Rule 1 of the Practical Guide as fulfilment of the conditions stipulated in sections 24 and 25 of the DPA. Section 24(1) states, 'no personal data shall be processed, unless the data controller has obtained the express consent of the data subject.' However the rest of the subsections in section 24 provide exceptions where in the absence of consent, personal data can be processed. These are situations where processing is necessary for performance of a contract to which the data subject is a party; in order to take steps required by the data subject prior to entering into a contract; in order to comply with any legal obligation to which the data controller is subject; to protect the vital interest of the data subject; for administration of justice; or in the public interest.

Section 25 provides the conditions when processing sensitive personal data. These are construed in the Practical Guide to be over and above the conditions provided in section 24 of the DPA. Section 25(1) states that no sensitive personal data shall be processed unless the data subject has (a) given his express consent to the processing of the personal data; or (b) made the data public. Section 25(2) clearly states that the conditions in section 25(1) shall not apply in stipulated situations: where processing is necessary for purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with his employment; in order to protect the vital interests of the data subject or another person where

consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; in order to protect the vital interests of another person, in case where consent by or on behalf of the data subject has been unreasonably withheld; for the performance of a contract to which the data subject is a party; in order to take steps required by the data subject prior to entering into a contract; or for compliance with a legal obligation to which the data controller is subject. Other conditions apply where processing is carried out by any entity or any association which exists for political, philosophical, religious or trade union purposes in the course of its legitimate activities and the processing is carried out in accordance with the Act; relates only to individuals who are members of the charitable entity or association; and does not include disclosure of the personal data to a third party without the consent of the data subject. Also processing of sensitive personal data is permitted in respect of the information contained in the personal data made public as a result of steps deliberately taken by the data subject; or is required by law.

It is imperative to note that sections 24 and 25 of the DPA refer to express consent. According to the Practical Guide, the notion of express consent means voluntary agreement to some act, practice or purpose. In this way, consent entails knowledge of the matter agreed to, and voluntary agreement. By 'express' it means consent which is given explicitly, either orally or in writing. However, no age limit is associated with consent.

From the above, it can be submitted that the classification of 'fairness' into 'fair collection' and 'fair processing' is oversimplification of the concept of 'processing'. The latter notion is broader. Under section 2 of the DPA 'processing' entails collection and various manipulations of personal data. The overall implication of this classification is to make the implementation of the DPA difficult. Moreover 'consent' is singled out as the primary condition for making processing fair. The other conditions are regarded as exceptions. As a result, this may affect the fair balance between the interests of the data subject and those of the controllers. In the European Directive, 'consent' and the other conditions are treated as equal in Art 7.

The other point to mention is that, the Practical Guide does not explain what is meant by 'lawfully'. Yet, there is no challenge in understanding it partly because in its wider sense 'lawfully' may mean processing that is in compliance with the provisions of the DPA. This may include elements of authorisation (e.g. consent) as legal justification for processing personal data. Similarly, the interpretation of 'lawfully' can be infused in the criterion of fairness.

The 'Second principle' states that personal data shall be obtained only for any specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose. This principle is partly reflected in sections 22(1), 26(a),(b) and 29 of the DPA. Rule 2 of the Practical Guide which interprets the second principle prohibits collection of information about people routinely and indiscriminately, without having a sound, clear and legitimate purpose for so doing. Data controllers can only process personal information against the purpose for which they registered in the entry of public register. Furthermore, Rule 4 of the Practical Guide lays down the test for 'compatibility'. This is whether 'you use and disclose the data in a way which those who supplied the information would expect it to be used and disclosed'. The Practical Guide gives some illustrations of the test. For example, transmission of personal information to the controller's agents who carry data operation on behalf of such controller and not retaining it for their own purpose, do not constitute 'disclosures' of data for the purposes of the Act.

The 'Third principle' is that personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed. This principle is also reflected in section 26(c) of the DPA. Rule 7 of the Practical Guide elaborates the third principle to mean that the data controller should only collect and keep enough information that enables him or her to achieve the purpose for which information is collected and no more. The controller is prohibited to collect and keep information 'just in case' a use can be found for the data in the future. Moreover, controllers are prohibited from asking intrusive or personal questions, if the information obtained in this way has no bearing on the specified purpose for which he or she holds personal data.

The 'Fourth principle' states that personal data shall be accurate and, where necessary, kept up to date. This principle appears also as an obligation in section 23 of the DPA. A close look indicates that it relates to the previous three principles. Rule 6 of the Practical Guide provides that a data controller after being informed as to the inaccurateness of personal data by a data subject must rectify, block, erase or destroy the data as appropriate. This obligation extends to the third party. If the data controller fails to rectify, block, erase or destroy inaccurate personal data, a data subject may apply to the Commissioner to have such data rectified, blocked, erased or destroyed. Rule 6 provides further that this requirement (i.e. keeping data accurate and up-to-date) has an additional importance in that it may result into liability of a data controller to an individual for damages if the former fails to observe the duty of care provision in the Act applying to the

handling of personal data. It is interesting to note that only Rule 6 of the Practical Guide and 'Your Rights'[1605] make reference to the remedy of damages. This is not repeated in the DPA, and in fact it was an issue of concern during parliamentary debates.[1606] Yet it was indicated that such a remedy may still be available under other pieces of legislation following the due process of law.[1607]

The 'Fifth principle' states that personal data processed for any purpose shall not be kept longer than is necessary for the purpose or those purposes. This principle is otherwise known as retention of personal data. It is reflected in sections 26 (d) and 28 of the DPA. Rule 8 of the Practical Guide provides that this requirement places a responsibility on data controllers to be clear about the length of time for which the data will be kept and the reason why the information is being retained. If there is no good reason for retaining personal information, then that information should be routinely deleted. Moreover, if the data controller would like to retain information about customers to help provide better service to them in future, he or she must obtain the customers' consent in advance.

The 'Sixth principle' is that personal data shall be processed in accordance with the rights of the data subjects under this Act. This principle has to be read in conjunction with Part VI of the DPA which deals with the rights of data subjects. The right of access to personal data under section 41 is the most important to the exercise of other rights of rectification, blockage, erasure or destruction in section 44 of the PDA. Rule 10 of the Practical Guide repeats essentially the requirements and exceptions provided in Part VI of the DPA. Moreover it places an obligation on the data controller to explain to the data subject the logic used in any automated decision making process where the decision significantly affects the individual and the decision is solely based on the automated process. Surprisingly, the DPA itself does not contain any clause on automated decision making similar to Directive 95/46/EC. It is doubtful if the Data Protection Commissioner can legally supply a new requirement not completely envisaged under the DPA.

Moreover, the exercise of the right of access is under condition to pay fee by the data subject to the controller. This fee is currently fixed at Rs 75(approximately US Dollar 2.5). With an 8% of population living below the poverty line in Mauritius,[1608] the fee requirement may present

[1605] Mauritius Data Protection Office, 'Data Protection-Your Rights -Volume 3', p.17.
[1606] Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No.XV of 2004), pp.105 and 111.
[1607] Ibid, p.111.
[1608] CIA WorldFactbook, 'Mauritius Population below poverty line(as of 9th January 2012),

unnecessary financial burden on the data subject henceforth a technical denial to access. This may also be the case to the rest of the population where a data subject makes many requests to different data controllers holding his or personal data. It may similarly cause financial burden where the same data subject makes multiple requests of information about him or her to the same data controller.

Apart from fee requirement, there are obstacles to the exercise of the right of access. Section 43(5),(a),(i) of the DPA exempts a data controller from providing access right to a data subject 'where he is being requested to disclose information given or to be given in confidence for the purposes of the education, training or employment, or prospective education, training or employment, of the data subject'. This leads to exclusion from the right of access regime in a range of processing operations carried out by schools, universities and employers.[1609] The rationale behind such exemption is not discussed in the preparatory works. This raises serious questions about its appropriateness.[1610] The other access denying provision is section 47 of the DPA relating to health and social work (see 5.4.2.3).

Also pertinent to mention is that the right of access and other data subject's rights are covered by the other code of practice 'Your Rights'. Hence the 'Sixth principle' has to be read together with this code of practice. Since some of the important issues already addressed above repeat themselves in 'Your Rights', detailed discussed is skipped here.

The 'Seventh principle' states that appropriate security 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. This principle is broadly covered in section 27 of the DPA as part of obligations of a data controller. However sufficient details of security measures are provided in Rule 5 of the Practical Guide. These include regular review of the security measures; weighing up the costs of security measures against the other factors; assessing the state of technological development; training of staff; using of contractual obligations to put processors under compliance to application of appropriate security measures; providing appropriate access control; and physical security.

---

https://www.cia.gov/library/publications/the-world-factbook/geos/mp.html last visited 26/03/2012.
[1609] Gayrel, note 1601, supra.
[1610] Ibid.

The 'Eighth principle' states that personal data shall not be transferred to another country, unless that country ensures an adequate level of protection of the rights of data subjects in relation to the processing of personal data. This principle has to be read with section 31 of the DPA. The latter section deals with international transfer of personal data similar to Arts 25 and 26 of Directive 95/46/EC. It is worth noting that the 'Eighth principle' is also dealt under Rule 9 of the Practical Guide.

The regime of international transfer creates conditions for Mauritian data controllers to transfer personal data to other countries. The primary requirement under section 31(1) of the DPA is that 'subject to subsection 2, no data controller shall, except with the written authorisation of the Commissioner, transfer personal data to another country.' The exceptions to section 31(1) are provided in section 31(2). The latter are similar to what the European Directive 95/46/EC provides in Art 26. Section 31(2) states that 'the Eighth data protection principle specified in the First Schedule shall not apply where (a) the data subject has given his consent to the transfer; (b) the transfer is necessary (i) for the performance of a contract between the data subject and the data controller, or for the taking steps at the request of the data subject with a view to his entering into a contract with the data controller; (ii) for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered at the request of the data subject, or is in the interest of the data subject, or for the performance of such a contract; (iii) in the public interest, to safeguard public security or national security; (c) the transfer is made on such terms as may be approved by the Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.'

Section 31(3) states that, 'for the purpose of subsection 2(c), the adequacy of the level of protection of a country shall be assessed in the light of all the circumstances surrounding the data transfer, having regard in particular (a) the nature of the data; (b) the purpose and duration of the proposed processing; (c) the country of origin and country of final destination; (d) the rules of law, both general and sectoral, in force in the country in question, and (e) any relevant codes of conduct or other rules and security measures which are complied with in that country'.

Rule 9 of the Practical Guide interprets the 'Eighth principle' together with section 31 as setting out two criteria for transfer of personal data to a foreign country: that the foreign country in question ensures an adequate level of data protection and also the transfer is authorised in writing by the Commissioner. The two conditions must exist simultaneously. This interpretation

appears to be correct particularly when one reads the first sentence of section 31(2) of the DPA. This opening sentence states categorically that the 'Eighth principle' shall not apply in all cases falling under that subsection. Concomitantly, it leaves the 'Eighth principle' to be applicable only in the context of section 31(1) of the DPA henceforth limiting the two stated conditions for transfer of personal data in that subsection. However, these conditions do not completely apply in the context of section 31(2) of the DPA. This is because transfer of personal data to a foreign country can still take place without adequate level of protection being afforded by such a country and without the written authorisation of the Data Protection Commissioner. This formulation is similar to Article 26 of the European Directive 95/46/EC. Yet, this view is contrary to the opinion of Gayrel who holds that 'a transfer is also possible in specific cases (exemptions), which however do not exempt the data controller from obtaining the approval of the Data Protection Commissioner.'[1611] As a result of this requirement, she argues, 'the Mauritian regime therefore appears to be quite restrictive with respect to transborder data flows. It requires the controller to obtain the approval of the Data Protection Commissioner in all cases, whether the transfer is intended towards a country ensuring an adequate level of protection or not. This appears to be burdensome both for controllers and the Commissioner.'[1612] Gayrel's position is largely influenced by a similar view taken by the Data Protection Commissioner in the Practical Guide particularly Rule 9 as well as her presentation of 5 October 2011. In such presentation the Commissioner raised the following question: what are the conditions to be fulfilled for transfers of personal data from Mauritius? She replied:-

> 'All transfers are subject to the written authorisation of the Commissioner. An application form is available on the homepage of the website to facilitate the request for authorisation. Transfers to countries <u>not</u> ensuring an adequate level of protection standards are further subject to conditions that may(sic) imposed by the Commissioner for protection of personal data involved.'[1613]

Gayrel and Commissioner's views over the Mauritian international transfer regime are erroneous for three reasons. First, both of them have omitted to interpret the phrase 'subject to' appearing in the beginning of section 31(1) of the DPA. Such a phrase has the effect of making section 31(2) of the DPA prevail over section 31(1), at least in those specific circumstances. Accordingly, the requirements of written authorisation by the Commissioner as well as the adequacy level of

[1611] Gayrel, note 1588, supra.
[1612] Ibid.
[1613] Madhub, note 1566, supra.

protection in the 'Eight principle' of data protection are excluded in the application of section 31(2) of the DPA. Second, the Mauritian Parliamentary debates (*Hansard*) surrounding section 31 of the DPA are quite clear that there are circumstances where transfer of personal data outside Mauritius do not require authorisation of the Commissioner. To be sure part of these debates reads:-

> 'Similar safeguards have also been provided under clause 31 of the Bill to prohibit the transfer of personal data to a third country without the written authorisation of the Commissioner. Thus, in accordance with the Eighth Data Protection Principle, the Commissioner will have to ensure that the transfer of personal data to a third (sic) country may only take place if the third (sic) country in question ensures an adequate level of protection, both in terms of disclosure of personal data to a third party and protection afforded to the data subject.'[1614]

It can be ascertained from the above paragraph that it was the intention of the Parliament that the transfer of personal data regime to a foreign country should not impede flow of information. That is why those exceptions were envisaged by the DPA. Third, the misinterpretation of section 31(2) of the DPA by both Gayrel and the Commissioner has been partly attributed by two other factors. The Commissioner has completely omitted to refer to section 31(2), (c) of the DPA in her Practical Guide. She just considered section 31(2), (a) and (b) as exceptions to section 31(1). This is also the case with Gayrel. However for Gayrel it appears that the word 'approved' used in section 31(2),(c) is similar to 'written authorisation' in section 31(1) of the DPA. This might not be correct because section 31(3) provides that 'adequate safeguards' referred in section 31(2),(c) of the DPA must be assessed at a country level to see whether such country provides an adequate level of protection of personal data. The criteria for assessment are then provided. Such criteria are almost the same as those provided in Art 25(2) of the European Directive 95/46/EC. Thus, the word 'approved' in section 31(2), (c) must be associated with the authority assessing the level of data protection in a country. However once such assessment has been conducted and a country approved as providing an adequate level of protection, transfer can always proceed without any further 'written authorisation' in section 31(1) of the DPA. This interpretation is in accord with the 'safeguards' referred in the above quoted paragraph from the *Hansard*. Yet, it

[1614] Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004), p.81.

must be admitted that the formulation of section 31 of the DPA is somewhat confusing. It was/is not proper to treat section 31(2), (c) as a rule of exception rather as a general rule as it is the case with the European Directive. The confusion is further exacerbated by the exclusion of the 'Eighth principle' at the beginning of section 31(2) of the DPA while at the same time referring to it in section 31(2)(c) and 31(3) which are meant to be exceptions for transferring personal data to a country without an adequate level of protection.

Apart from the eight data protection principles, the DPA contains special rules for processing of personal data. These include sensitivity (already considered above); direct marketing; and data matching.

Section 30 of the DPA governs processing of personal data in the context of direct marketing. Generally, this provision does not prohibit direct marketing neither does Rule 12 of the Practical Guide on direct marketing. Section 30(1) of the DPA only states, 'a person may, at any time, by notice in writing, request a data controller (a) to stop; or (b) not to begin, the processing of personal data in respect of which he is a data subject, for purposes of direct marketing.' Once the data controller receives such notice he is obliged under section 30(2) to act within a period of 28 days by either erasing the data if such data were kept only for purposes of direct marketing; and where the data were kept for direct marketing and other purposes, stop processing the data for direct marketing. Further, the data controller is required to notify the data subject in writing of any action taken.[1615] Where the data controller fails to comply with a notice issued by the data subject, the latter may appeal to the Tribunal.[1616] In event the data controller fails to comply with an order of the Tribunal he or she shall commit an offence.[1617]

According to the Commissioner, the application of the data protection law in the sector of direct marketing varies depending on the medium through which the marketing is delivered.[1618] Thus, there are marketing by post, phones, fax and e-mail. Postal marketing is the traditional and oldest form of marketing for mail received through a person's letter box.[1619] To be considered direct marketing, a mail must be addressed to a named person and must be promoting a product or

[1615] Mauritius Data Protection Act 2004, s. 30(4).
[1616] Ibid, s. 30(5).
[1617] Ibid, s.30(6).
[1618] Mauritius Data Protection Office, 'A Practical Guide for Data Controllers & Data Processors-Volume 1'-Rule 12.
[1619] Ibid.

service.[1620] In the Commissioner's view an unaddressed mail put into a letter box or mail addressed to the 'occupant', 'the resident' or 'the householder' does not necessarily involve the use of personal data and consequently data protection legislation may not apply.[1621] While the DPA is silent about consent for purposes of direct marketing, Rule 12 of the Practical Guide provides two main forms of consent at least with regard to postal marketing. These are 'opt in' or 'opt out'. The former is a box which invites a person to indicate if he or she would like to receive such material. Unless he or she demonstrates 'active consent' by ticking the box, his or her personal data cannot be used for direct marketing purpose. On the other hand, an 'opt out' box invites a person to indicate (usually by ticking) if he or she objects to receive direct marketing material. According to the Commissioner, failure by the person to tick the box, may be taken as an indication of his or her 'passive consent' to receive the direct marketing material. The Commissioner indicates in the Practical Guide that she is prepared to accept that the individual has given his or her 'passive consent' by not ticking the 'opt out' box, provided the personal data in question are not of a sensitive nature. Moreover, the Practical Guide is clear that consent may also be verbal or if a person participates in a special promotion, which clearly involves the use of personal data for certain clearly defined direct marketing purposes, participation may be taken as implicit consent by individual. Also significant, Rule 12 of the Practical Guide provides that a person intending to use personal data for direct marketing purposes should offer a cost free opt-out facility. This requirement applies across all other forms of communications. Other important rules of postal direct marketing include the following:-a controller is prohibited from using personal information obtained in the past for a different purposes for direct marketing; a person cannot sell a list of personal data for direct marketing unless he or she obtains the consent of all the individuals affected; consent from children should be obtained through their parents or guardians; and ordinarily a controller is not allowed to direct market at people referred by his or her existing customers.

As to residential subscribers' phone calls and faxes; these are prohibited unless the controller obtains prior consent from the individuals concerned. This applies also to business subscribers' phones and faxes. However, in case of directing marketing by using e-mail, the controller must obtain an individual's consent or he/she obtained those information in the course of a sale to him or her for a service or product; the controller disclosed his or her identity, the purpose of collecting personal data; the persons or categories of persons to whom such personal data may be disclosed and any other information which is necessary so that processing may be fair; also

[1620] Ibid.
[1621] Ibid.

the direct marketing the controller is sending is in respect of his or her similar products and services only; the controller had given a simple cost-free means of refusing the use of an individual's contact details for direct marketing and such individual did not object and he or she was given similar options subsequently still he or she could not refuse.

Section 32 of the DPA generally prohibits data matching. However there are exceptions where data matching is permissible: where the data subject has given his consent; the Commissioner has consented to the procedure being carried out and such procedure is carried out in accordance with conditions imposed by the Commissioner; or data matching is required or permitted under any other enactment. Rule 13 of the Practical Guide clearly provides that any data matching that is likely to adversely affect the data subject must be carried out only after the data subject and Commissioner have consented.

5.4.2.5 Data Protection Commission

The Data Protection Commission is the main institution of enforcement of the Data Protection Act 2004. It is established under section 4(1). Structurally the Commission falls under the Prime Minister's Office. It is composed of the Commissioner as its head and other public officers.[1622] To qualify as the Commissioner one must be a barrister with at least five years standing at the Bar.[1623] While the Act is silent as who appoints the Commissioner, the Website of the Commission provides that the Data Protection Commissioner is appointed by the Public Service Commission.[1624] Moreover, the Data Protection Act does not state the length of tenure of the Commissioner and if he or she can be reappointed. As regards the other public officers in the Data Protection Commission, the Act does not specify their numbers. Neither does it list their respective positions nor qualifications, leave alone their remunerations. However such officers are under direct administrative control of the Commissioner.[1625] In her first Annual Report 2009-2010, the Commissioner made a call that 'it is further of utmost importance that this office be provided within the least possible delay with adequately qualified staff to carry out the activities listed in section 5 of the Data Protection Act.'[1626] She also requested the Prime Minister's Office

[1622] Mauritius Data Protection Act 2004, ss. 4(2) and 4(4).
[1623] Ibid, s.4(3).
[1624] Mauritius Data Protection Commission's Website, http://www.gov.mu/portal/site/dataprotection/menuitem.00d90163887e1852a6a4bc10a0208a0c/, last visited 27/03/2012.
[1625] Mauritius Data Protection Act 2004, s.5 (5).
[1626] Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010, p.2.

to consider appointing on a contract of one year under the capacity building programme foreign consultants with expertise in data protection so that they can train the staff once recruited and also assist the Commission in the performance of its duties.[1627] These requests by the Commissioner leave a lot to be desired on the qualifications of members of the Commission.

Before assuming duties, the Commissioner and every officer of the Commission is required under section 6 of the DPA to take oath. The oath puts the Commissioner and other officers in the Commission under duty of confidentiality. They are therefore not required to divulge any information obtained in the exercise of a power or in the performance of a duty under the Act. However section 6 permits divulge of information in accordance with the provisions of the DPA, any other enactment, upon a court order, or as authorised by the order of a Judge. As it will be shown subsequently, this provision has ramification in reporting decisions of complaints by the Commissioner.

The question whether or not the Mauritian Data Protection Commission is independent is difficult to assess. Yet in theory the general view is that the Commission is independent. This general view comes following the amendment of the Data Protection Act 2004 on 15 April 2009 through the Stimulus Package Act 2009. The latter legislation repealed section 21 of the DPA. To be sure, section 21 provided:-

> '21(1) Subject to subsection (2), the Prime Minister may give in writing such directions of a general character to the Commissioner, not inconsistent with this Act, which he considers to be necessary in the public interest, and the Commissioner shall comply with those directions.
>
> (2) The Prime Minister shall not (a) give any direction in relation to any specific matter which is the subject of any investigation by the office; and (b) question the Commissioner or an authorised officer, or otherwise enquire into, a matter which is under investigation by the office.'

Subscribing to the above view, Gayrel argues that the repeal of section 21 of the Data Protection Act 2004 shows the will of the Mauritian legislature to provide an unambiguous independence to the Commissioner.[1628] However repeal of section 21 of the DPA may not necessarily translate

[1627] Ibid, p.14.
[1628] Gayrel, note 1588, supra.

independence of the Commission into practice although it is admitted this is a sound starting point. As analogously argued by Professor Michelo Hansungule:-

> 'As indicated, Angola, Botswana, Malawi and most other Southern African constitutions recognize and guarantee the notion of judicial independence. Surprisingly, Mauritius, one of the most widely acclaimed democracies in Africa throughout the period of one party dictatorships, does not have an explicit pro-judicial independence clause in its Constitution. There are typical provisions one finds in a constitution describing the structure of government including judicial structures in the Constitution of Mauritius but the document is shy to pronounce itself on the specific issue of judicial independence. What this means is that while a country may not make special mention of judicial independence in its constitution, it may achieve it in practice. In other words, it is not enough to proclaim the independence of the judiciary for the judiciary to be independent. Much more will need to be done to actually achieve the standard in practice and a statutory proclamation to that effect though a desired natural first priority especially for countries emerging from the throes of dictatorships, nevertheless, does not achieve it by itself.'[1629]

In the context of judiciary other safeguards exist (e.g. security of tenure for judges) in which case the absence of explicit proclamation of independence of judiciary may not affect it in practice. However such safeguards are lacking with the Commission. For example, the Data Protection Act does not contain the compatibility regime which addresses the conflicts of interests between members of the Commission and the executive. Similarly the DPA does not state expressly that the Commissioner is independent such that the Commissioner may offer any opinion even if it is unfavourable to the public sector. This is contrary to Art 28(1) of the European Directive 95/46/EC which explicitly makes reference to 'complete independence'. Yet this omission is partly mitigated by section 60 of the Act which limitedly provides for immunity of the Commissioner and authorised officers against civil and criminal liability. Moreover, there is no provision in the DPA stating the source of funds for the activities of the Commission.

Worthwhile to mention is that section 21 of the DPA raised fierce debates during Parliamentary discussions of the Data Protection Bill 2004. On the one hand, the government, through the

[1629] Hansungule, M., 'Independence of the Judiciary and Human Rights Protection in Southern Africa', pp.1-9, p.6, http://www.pdfcari.com/Judiciary-and-Human-Rights.html last visited 29/03/2012.

Prime Minister, maintained that it was necessary for him to have powers to give directions to the Commissioner on account of national security.[1630] On the other hand, parliamentarians objected such a provision on account of potential abuse.[1631] The parliamentarians cited three illustrations of possible abuses of such powers. The first involved an occasion where sensitive personal information was released when the Prime Minister attended a socio-cultural organisation.[1632] The other relates to section 45 of the Bill (the same as the DPA) which gives the Prime Minister power to exempt from application of the Act any of its provision based on national security.[1633] The third instance likely to operate in undermining the independence of the Data Protection Commissioner is assessed from the entire past experience of the public service in Mauritius as aptly posited by Dr. Ramgoolam, 'we have seen in the past that some people do not feel that independence. They don't have independence to act independently and I think this is the danger we face.'[1634] With this last illustration, it can be submitted that sometimes informal directives from the executive may partly be the reason for fear to act independently. However and as submitted above, it is difficult to trace such kinds of directives as they are given secretly.

Section 5 of the Data Protection Act vests the Commissioner with a wide range of functions typical of any data protection authority. These include ensuring that subjects of the Data Protection Act comply with its provisions and any regulations made under it; to issue or approve codes of practice or guidelines for the purposes of the Act. This function is further consolidated in section 56 of the Act; to create and maintain a register of all data controllers and data processors; to exercise control on all data processing activities, either of its own motion or at the request of a data subject, and verify whether the processing of data is in accordance of the DPA or regulations made under it; to promote self-regulation among data controllers and data processors; to investigate any complaint or information which give rise to a suspicion that an offence, under the Act may have been, is being or is about to be committed; to take such measures as may be necessary so as to bring to the knowledge of the general public the provisions of the DPA; to undertake research and monitor developments in data processing and ensure that there are no significant risks of any adverse effects of those developments on the privacy of the individuals; to examine proposals for data matching or linkage and ensure that they do not cause any adverse effects to individuals privacy; to co-operate with supervisory

[1630] Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004), pp.80 and 112.
[1631] Ibid, pp.86, 87 and 108.
[1632] Ibid, p.87.
[1633] Ibid.
[1634] Ibid, p.108.

authorities of other countries, to the extent necessary for the performance of his duties under the Act particularly by exchanging relevant information in accordance with any other enactment; and to do anything incidental or conducive to the attainment of the objects and better performance of his duties and functions under the DPA. The Commissioner is also required under section 55 of the DPA to prepare and submit to the National Assembly annual report of the Commission's activities not later than three months of every calendar year. Matters to be reflected in the report include a statement about the operation of approved and issued codes of practice; other matters; and any recommendations that the Commissioner thinks fit in relation to the implementation of the Act, and in particular the data protection principles.

In exercise of the above functions, the Commissioner is vested with various powers. Generally, the Commissioner has powers to do anything for the purpose of carrying out his functions as long as it appears to him to be requisite, advantageous or convenient for discharging such functions.[1635] Apart from these general powers, the Commissioner has specific powers to certain acts under the DPA. It may appear that the specific powers were intended to operate in specific contexts. Yet beyond those contexts, it is difficult to see how the powers of the Commissioner may be invalid given that under section 7 of the DPA he has the general powers to do anything as long as they are tandem to the implementation of the Act. To be sure, specific powers vested in the Commissioner relate to the following:-powers to obtain information (section 8). However the exercise of such powers is subject to certain provisions of pieces of legislation listed there. The Commissioner may delegate his powers to any officer in his office or any police officer on his or her behalf.[1636] Such powers are limited to those relating to investigation and enforcement powers but nothing more. In relation to dispute settlement, where a complaint has been made to him, the Commissioner is empowered to investigate the complaint unless he is of the opinion that such complaint is frivolous or vexatious.[1637] And, as soon as practicable, he is required to notify the complainant in writing of his decision in relation to the complaint.[1638] Moreover, the notice by the Commissioner to the complainant must explain to him that if he is aggrieved by the Commissioner's decision, he has the right of appeal to the ICT Appeal Tribunal.[1639]

To give effect to functions vested in him, the Commissioner has power to serve an enforcement notice under section 12 of the Data Protection Act 2004. This notice can only be issued where

[1635] Mauritius Data Protection Act 2004, s.7.
[1636] Ibid, s.9.
[1637] Ibid, s.11 (a).
[1638] Ibid, s.11 (b).
[1639] Ibid.

the Commissioner is of the opinion that a data controller or processor has contravened, is contravening or is about to contravene the provisions of the DPA. The role of the enforcement notice is to direct the data controller or processor to take specific steps within such specified time in the notice. Failure to comply with the enforcement notice without reasonable excuse is an offence which upon conviction attracts a fine not exceeding 50,000 rupees(approximately US Dollar 1,660) and to imprisonment for a term not exceeding two years. Once complied with the enforcement notice, the data controller or processor is required to notify the data subject concerned. It is imperative to note that the enforcement notice does not bar the Commissioner from investigating the same matter he has called the data controller or processor to comply. Where the data controller or processor is aggrieved by the enforcement by the Commissioner he may appeal to the ICT Appeal Tribunal. The Commissioner has also powers to seek expeditiously for preservative order from a Judge in Chambers where he has reasonable ground to believe that such data is vulnerable to loss or modification.[1640]

Other categories of powers vested in the Commissioner include power to carry out prior security checks(section 14); power to carry out periodic audits of the systems of data controllers or processors to ensure compliance to the data protection principles(section 15); and powers to request assistance for purposes of gathering information or proper conduct of investigation (section 16). Also, to better enable the Commissioner to discharge his duties, the Data Protection Act vests in him under section 17 powers of entry and search any premise. However, before the Commissioner exercises such powers, usually through an authorised officer, he must apply and obtain a warrant from a Magistrate. Moreover before entry and search, the authorised officer must show the owner or occupier a warrant issued by the Magistrate which is only valid for the period specified and other conditions stipulated there. It is an offence for the owner or occupier of a premise to obstruct the authorised officer to enter and search if the warrant is shown to him or her.[1641] Finally, the Commissioner has powers to refer the matter to the police following a revelation of commission of offence from his investigation.[1642]

The above outlined functions and powers of the Commissioner are similar to those provided in Arts 27 and 28 of the European Directive. However, it is important to assess how they have been implemented in practice. One caveat must be pointed out in relation to this assessment. Most of the provisions with regard to functions and powers of the Commissioner are

[1640] Ibid, s.13.
[1641] Ibid, s.19.
[1642] Ibid, s.21.

interrelated and overlap in their implementation. As a result, in order to keep focus, key areas of exercise of these functions and powers are discussed. These include public awareness of the provisions of the Data Protection Act 2004, issuance or approval of codes of practice or guidelines, determination of complaints and preparing annual reports.

- **Public Awareness**

As pointed out in 5.4.2.2, there was no or little public consultation of the Data Protection Act 2004 during its legislative process. To partly mitigate the implications of such an omission, the Act incorporates a provision on carrying public awareness of DPA and its regulations as part of the functions of the Commissioner. However, it should be clear that the provision on public awareness was not specifically inserted to address the omission to consult the public prior to the adoption of the DPA. Instead, it was incorporated to facilitate compliance to the law by data controllers and subjects just as it is the case elsewhere.

In discharging her duty to bring into the knowledge of the public the provisions of the Data Protection Act and its regulations under section 5(g), the Commissioner had issued a leaflet on data protection to individuals and organisations. The leaflet is about their obligations and rights. The leaflet is also available on the Commission's homepage of its website. Perhaps the most important efforts by the Commissioner in sensitising the public about the Data Protection Act are demonstrated by handful of presentations delivered to various sectors: banks, business processing outsourcing sectors and employers including universities.[1643] All the presentations of the Data Protection Commissioner are posted on PowerPoint on the 'presentation' section of the website of the office.[1644] Currently there are twenty five(25) presentations (up to 26 May 2012).[1645] Apart from these presentations, the Commissioner has further developed a '*teens corner*'

[1643] Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010, p.6.
[1644] Ibid, p.34.
[1645] 'Overview of the Mauritian Data Protection Act' presented on the occasion of the Cyber Security Conference by the Commissioner 30 November 2007; 'The challenges imposed by biometric technology on data protection and privacy' presented on 1st of December 2008 on the occasion of the Computer Security Day 2008; 'A simplified understanding of the intricacies of the Data Protection Act and how the implementation of this legislation will affect your daily life' presented on 27th of February 2009 for workshop on Privacy and Data Protection organised in collaboration with the National Computer Board; 'Overview of the legal requirements imposed by the Data Protection Act on data controllers and the corresponding rights of data subjects' presented on 10 March 2009 at the University of Technology to the students; 'An overview of the Data Protection Act and its implications as regards registration transfers of personal data and data subject access requests' for the banking sector presented by the Commissioner on the 5th June 2009 at the Mauritius Bankers' Association; 'The Data Protection Implications for our DNA Bill' presented by the Commissioner on the 9th June 2009 at the Awareness Workshop on Legal Aspects of the Use of Human DNA; 'An overview of the Data Protection Act and its implications as regards registration

which is found on the website of the Commission.[1646] The reason for developing this *corner* is to sensitise young people on the pros and cons of the social networking sites.[1647]

From the above observations, it can be submitted that the sensitisation of the Data Protection Act and its regulations is still severely limited. At present, the Commissioner's efforts to make the Data Protection Act and its regulations known to the public are confined largely to data controllers and processors. This is revealed in the Data Protection Commissioner's Second Annual Report where it states, 'the Data Protection Office has deployed considerable efforts to educate data controllers on their obligations under the Data Protection Act.'[1648] Similarly, one can still notice the limited level of sensitisation from the number of presentations so far made by the Commissioner. The 25 presentations made by the Commissioner are far smaller in number compared to the number of registered data controllers and processors by December 2010 which was 8200.[1649] This number might have gone higher in 2011. However, one can argue that other data controllers and processors can access the 25 presentations from the homepage of the

---

and data subject access requests for the Ministry of Information and Communication Technology' presented by the Commissioner on the 10th June 2009 at the Ministry of the Information and Communication Technology; 'Data Protection Requirements for the ITES/BPO/KPO/LPO sector' presented by the Commissioner on 03 September 2009 at MEF-MCCI Building, Ebene in collaboration with OTAM; 'Data Protection Implications for the Public Sector' presented by the Commissioner on 16 September 2009 at the Ministerial Security Committee in collaboration with the National Security Advisor's Office; 'Les Propositions apportées par la commissaire au projet de loi mauricien visant à protéger les enfants à l' ère numérique' presented by the Commissioner on 2 November 2009 at the Francophone Conference held in Madrid; 'Ensuring compliance with data protection principles from a practical perspective' presented by the Commissioner on 30 November 2009 on the occasion of the Computer Security Day 2009; 'A Legal Purview of the Data Protection Act and the Mission of the Data Protection Office' presented by the Commissioner on 26 January 2010 to Mauritius Employers Federation members; 'The Data Protection Act - An introduction to its implications and objectives' presented by the Commissioner on 13 August 2010 to the staff of the Local Government Service Commission; 'The Data Protection Obligations of a Public Institution' presented by the Commissioner on 5 October 2010 to the Ministry of Social Security at the Training Unit of the Ministry; 'The Obligations of a Public Data Controller and Processor under the Data Protection Act' presented by the Commissioner on 16 November 2010 to the Ministry of Health; 'Analysis of the Obligations of a Data Controller and a Data Processor' presented by the Commissioner on 11 November 2010 to Data Protection Compliance Officers organised by Geroudis Management Services Ltd; 'How to Ensure Effective Compliance with the Data Protection Act' presented by the Commissioner on 18 January 2011 to Lamco Insurance Ltd; 'Making Sense of it:- What is Data Protection?' presented by the Commissioner to the Truth and Justice Commission on 09 March 2011; 'How to incorporate data protection rules to safeguard shareholders' personal data of the sugar investment trust' presented by the Commissioner on 25 March 2011; 'Data protection from an employment perspective' presented by the Commissioner on 05 July 2011 to Groupe Mon Loisir Ltd; 'Video on Data Protection' presented by the Commissioner on 12 August 2011 to International Card Processing Ltd and others; 'La problématique juridictionnelle et les enjeux du transfert de données personnelles dans les opérations d'externalisation' presented by the Commissioner on 21 September 2011 to AFAPDP in Dakar; 'The Data Protection Office in Mauritius - The Challenges Ahead' presented by the Commissioner on 5 October 2011 to ICT-BPO Forum; 'Overview of the Fundamental Aspects of the Right of Access' presented by the Commissioner on 20 April 2012 to Mutual Aid Association Staff; and 'Data Protection Fundamentals for the Banking Sector' presented by the Commissioner on 26 April 2012 to Barclays Bank.

[1646] Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010, p.34.

[1647] Ibid.

[1648] Mauritius Data Protection Office, Second Annual Report of the Data Protection Commissioner January 2010-December 2010, p.6.

[1649] Ibid, p.9 (number of registered data controllers and processors).

Commission's website. Given the fact that data protection is a new field of law, the direct interaction of the Commissioner and data controllers and processors is necessary for clarifying the understanding of various concepts, obligations and rights defined in the Act and its regulations. On the other hand, the effectiveness of the leaflet distributed by the Commissioner is difficult to assess. In the first place, it is difficult to ascertain how many data controllers, processors and individuals received such a leaflet. Moreover, it is difficult to assess if those who received the leaflet were able to understand it without difficulties.

Another point needing comment is the availability of various documents on data protection on the Commission's website. Admittedly any person in Mauritius and outside may at any time access such documents to familiarise with the operation of the Data Protection Act and its regulations. However, it has been shown in 5.2 that only 31.7% of Mauritians had access to the Internet by 2011. This number is relatively small as a result the limitation posed by Internet penetration has adverse impact in the use of such medium to reach a large number of public. Moreover, out of this number it is less clear how many teens have access to the Internet in Mauritius.

Despite the above efforts to educate the public and certainly due to lack of effective mechanisms for that purpose, the Commissioner has identified 'continued lack of awareness amongst data controllers and data processors of their data protection obligations'[1650] and ' continued lack of awareness on the part of the members of the general public(who, as a result, give away their personal information too easily, do not ask why personal information is needed or fail to 'tick the box' to say they do not want to be contacted)[1651] as among the nine threats to data protection in Mauritius.

- **Codes of Practice and Guidelines**

The Commissioner issued various codes of practice and guidelines under the provisions of sections 5(b) and 56 of the DPA. Some of them have already been referred in various parts of this thesis. Yet, it is important to list these codes and guidelines so that a general assessment can easily be made. They include: A Practical Guide for Data Controllers & Data Processors-Volume 1; Registration Classification & Guidance Notes for Application of Data Controllers & Data

[1650] Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010, p.42.
[1651] Ibid.

Processors-Volume 2; Data Protection-Your Rights-Volume 3; Guidelines for Handling Privacy Breaches-Volume 4; Guidelines to regulate the Processing of Personal Data by Video Surveillance Systems-Volume 5; Guidelines on Privacy Impact Assessments-Volume 6; Practical Notes on Data Sharing Good Practices for the Public and Private Sector-Volume 9; and Code of Practice issued by the Data Protection Commissioner for CCTV Systems operated by the Mauritius Police Force.

The above codes of good practice and guidelines either supply details to the main provisions of the DPA or offer simplified version of the provisions of the Act to ease their understanding. Sometimes both aims manifest in the texts of these codes and guidelines at the same time. As alluded to, in some of the codes of good practice and guidelines, the Commissioner has supplied conditions for processing which somewhat appear in excess of the provisions of the DPA or which are sometimes in conflict with the principle Act. For example, the general condition of data processing in the DPA is data subject's consent under section 24(1). However the Act does not define what is an 'express consent'. It only defines 'consent' in section 2 as any freely given specific and informed indication of the wishes of the data subject by which he signifies his agreement to personal data relating to him being processed. As pointed out, in 'A Practical Guide for Data Controllers & Data Processors-Volume 1' the Commissioner has taken the view that 'express consent' is consent given explicitly, either orally or in writing. According to the Oxford Advanced Leaner's Dictionary[1652] the word 'explicitly' in relation to a statement or piece of writing denotes something which is clear and easy to understand. Yet, despite the clear requirement of 'express consent' in section 24(1) of DPA, the Commissioner has significantly lowered 'express consent' to 'passive consent' in the direct marketing context and is prepared to accept it in compliance to the law.[1653] The latter means that the data subject does not 'tick a box' in order to 'opt out'. Another instance where 'A Practical Guide for Data Controllers & Data Processor-Volume 1' provides a condition which is not stipulated in the DPA relates to the obligation imposed upon data controllers and processors to explain to data subjects the logic used in any automated decision making process where an individual is significantly affected.

The inconsistencies between the codes of practice and guidelines on the one hand and the DPA have not yet been considered by any court in Mauritius. However, it is doubtful if the former

[1652] Hornby, A.S., Oxford Advanced Learner's Dictionary of Current English, 7th Edition, Oxford University Press, New York, 2005, p.536.
[1653] See Mauritius Data Protection Office, A Practical Guide for Data Controllers & Data Processors-Volume 1, Data Protection Rule 12.

may pass the repugnancy clause in the Interpretation and General Clauses Act 1974.[1654] The repugnancy clause is provided in section 23(c) of the Interpretation and General Clauses Act. It states that where an enactment confers power on any person to make a subsidiary enactment for a general purpose and also for a special purpose, the special purpose shall not derogate from the generality of the power conferred by the general provision. Since there is no any court decision annulling provisions of the codes of the practice or guidelines, the Commissioner's opinion as contained in these legal texts comprises the correct statement of the law in Mauritius.

There is yet another problem with the codes of practice and guidelines. It is about the legality of their application. Section 56(3) (b) of the Data Protection Act 2004 states that any code of practice shall, where the code is approved under subsection(1), come into operation on a day specified by the Commissioner. In section 56(1) the Commissioner may 'issue or approve codes of practice' or 'issue guidelines'. Yet in section 5(b) it is provided that the Commissioner shall 'issue or approve codes of practice or guidelines' for the purposes of the DPA. While section 5(b) leaves it open for the Commissioner to 'approve' both the codes of practice and guidelines, section 56(1) restricts the term 'approve' to codes of practice as against 'issue' which is used for both codes of practice and guidelines. Interestingly, DPA does not distinguish a 'code of practice' from 'guideline'. However in practice the two appear closely related. For example the Guidelines to regulate the Processing of Personal Data by Video Surveillance Systems-Volume 5 is similar to the Code of Practice issued by the Data Protection Commissioner for CCTV Systems operated by the Mauritius Police Force. Yet, the former is a guideline while the latter is a code of practice. So far the Commissioner has only specified the date of commencement of the Code of Practice issued by the Data Protection Commissioner for CCTV Systems operated by the Mauritius Police Force and left the guidelines unspecified. Since both the codes of practice and guidelines are either issued or approved by the Commissioner under the same legal provision and also affect the data controllers, processors and data subjects, their commencement date is necessary to be given.

- **Complaints**

As pointed out, section 11 of the DPA gives the Commissioner power to receive and determine complaints. The Commissioner has decided seven complaints since 2009 to 24 May 2012. Such decisions have been posted on the section of the Commission's website called 'Decisions on

[1654] Mauritius Interpretation and General Clauses Act 1974(Act No.33 of 1974).

Complaints'. Postings appear to be made immediately after the decision. However, it is difficult to establish exactly the date as the website does not contain this information. Currently, the exact number of pending complaints is unknown since the Commissioner does not post such records on the website. However, during interview with the researcher of this thesis on 4 July 2011(Port Louis, Mauritius), she confirmed that there were thirteen pending complaints. This number may have arisen. However, four complaints were determined after the day of interview with the Commissioner.

To initiate a complaint, a complainant has to fill a prescribed off print or electronic form. The former can be downloaded from the Commission's homepage in the 'To report your complaint' section while the latter is available on 'Online submission of complaint'. In relative terms, the off print form requires the complainant to fill only little information: name of complainant; name of a person against the complaint; contacts of the complainant(address, e-mail address and phone number); address of the person against the complaint; nature of relation; date of submission; and brief facts about the complaint. On the other hand, the online form requires pre-registration to obtain a username and password. As a result, more information is needed: gender, age group, country, occupation, education, interest, and citizenship. However after logging in, the same form as off print appears for the complainant to fill.

In practice, a party lodging complaint is called 'complainant' while a party responding it is called 'respondent'. If there are more than one complainants or respondents, these are differentiated by numbers (e.g. complainant 1, 2, or respondent 1, 2). In the reported decided complaints, the identities of the complainant and respondent are always anonymised. The Commissioner has done so on the basis of a duty of confidentiality imposed upon her and every officer in the Commission under section 6 of the DPA. Thus, the section of 'Decisions on Complaints' bears the following notice:-

> 'Please note that all complaints lodged to the Data Protection Office under section 11 of the Data Protection Act are also subject to a duty of confidentiality imposed upon all officers of the Data Protection Office. The Commissioner has thus decided to publish decisions on this public website without revealing the personal data of the complainants and respondents to the public but only the decision based on the facts of the case.'

However, some non-direct parties to a complaint are fully named by their identities. This is the case with the third and fifth decisions considered below. Yet, in the seventh decision, the Commissioner avoided to mention the non-direct parties involved in the complaint.

The decisions are cited by reference numbers followed by 'In the matter of' then names of the parties. The first and second decisions are referenced as PMO/DPO/DEC while in the third to seventh DPO/DEC. In each case a serial number of a decision is added at the end. In these references PMO stand for Prime Minister's Office, DPO Data Protection Office and DEC decision. It is not clear why the Commissioner dropped PMO in the subsequent reporting of her decisions. One may argue, though with some risks of certainties, that the Commissioner wanted to demonstrate a sense of independence of her office in determining the complaints.

The other basic feature of the Commissioner's decisions is that they are relatively short usually ranging between two to three A4 pages. Yet, they are sufficient to convey information about the nature of a complaint, legal issues involved, essential steps taken by the Commissioner in investigation, summary of evidence, her findings and verdicts. However, in certain cases (e.g decision seven) these decisions are longer.

As pointed out, so far the Commissioner has decided seven complaints. It is imperative to survey these decisions in order to uncover: how the basic data protection principles have been applied in practice; how the Commissioner has engaged other provisions of the DPA, codes of practice and guidelines; how relevant are such decisions in the development of data protection system in Mauritius; at whose interests the decisions are made; etc. These decisions are considered in their order of reference numbers.

The first decision is *Complainant v Respondents 1, 2, and 3.*[1655] The complaint in this decision was lodged on 21 July 2010 at the Data Protection Office under section 11 of the DPA. It was about unauthorised use of the complainant's curriculum vitae (CV) by respondents 1, 2 and 3 which was originally communicated electronically to the respondent 1. The complainant alleged that he had a contract with respondent 1 for the implementation of a Food Security Management System (HACCP-MS 133) project at respondent 2 who was a beneficiary of respondent 3. According to the complainant, he cancelled his contract with respondent 1 for non-fulfilment of the terms of the contract. Following such cancellation, the complainant officially wrote to the

[1655] Ref.No:-PMO/DPO/DEC/1.

respondent 1 asking him not to use or process his CV. He further alleged that respondent 1 had acted in bad faith and breach of contract by using his curriculum vitae to obtain financial benefit for his client, namely respondent 2 from a public institution, namely respondent 3. The complainant also added that respondent 2 acted in bad faith by using his CV to obtain financial benefit from a public institution i.e. respondent 3. He also alleged that respondent 2 acted as an accomplice with its consultant i.e. respondent 1 to defraud the complainant. Lastly, he complained that respondent 3 had failed to recognise his right by not stopping to use his CV when asked to do so.

In her decision, the Commissioner found that there was no evidence to support the complaint of unauthorised or unlawful use of personal data in the complainant's CV by respondents 1, 2 and 3 in carrying out project HACCP-MS 133. The reason given by the Commissioner was that the complainant was not any more hired as consultant for the project after the cancellation of the contract with respondent 1. Moreover respondent 1 had informed respondent 3 that the complainant was not hired for the project. Also, the Commissioner's site visit at respondent 1's company premise, made with its consent, revealed no evidence of any personal data in the hard drive nor external media storage of the computer of respondent 1. The latter had deleted all personal data of the complainant suggesting that he had no intention to use it in future. However, the Commissioner requested respondent 3 in writing to return the complainant's CV through her office which he did guaranteeing that it was never used for the benefit of the project. Following the return of his CV, the complainant made a statement recorded by the Commissioner that since all respondents had endeavoured not to use it, he was satisfied with the outcome of the enquiry.

Based on the above, the Commissioner set aside the complaint under sections 26(a) & (b) and 28 of the Data Protection Act as the offence had not been proved beyond reasonable doubt. Moreover, the CV was not used or disclosed in any manner incompatible with the purpose for which data was collected and processed and was further kept only for the lawful purpose. When the purpose for keeping the data had lapsed, respondents deleted and/or removed all data pertaining to complainant within their possession. The Commissioner's decision was delivered on 23 March 2011.

The Commissioner's above decision is based on the second principle of data protection in the First Schedule of the Data Protection Act i.e. purpose specification. The latter principle

manifests as duty on use of personal data in section 26(a) & (b). Also important to note, the Commissioner's decision is based on the duty to destroy the personal data in section 28 of the DPA once its purpose has lapsed. Both of these requirements were fulfilled by the respondents. Yet, a close examination of the above decision leaves a lot to be desired. For example, it was until the complainant had brought the matter into the attention of the Commissioner and the latter had officially written the respondent 3, he was only able to return the complainant's CV. However evidence on record reveals that respondent 1 had already notified respondent 3 that the complainant was no longer hired as consultant of the project. Despite such notification respondent 3 continued to retain the complainant's CV. It can be submitted that respondent 3 did not comply with section 28 of the DPA. Moreover, it can be argued that the Commissioner omitted to consider the fifth principle of data protection principles in the First Schedule of the DPA on data retention. This principle manifests as an obligation on the party of data controller and processors in section 26(d). As alluded to, the Commissioner has taken the view in Rule 8 of 'A Practical Guide for Data Controllers & Data Processors-Volume 1' that the data controller must be clear about the length of time for which data is kept and the reason why the information is being retained. Had the Commissioner considered all these, she would have probably found respondent 3 in breach of his obligations under the DPA.

The second complaint considered by the Commissioner was *Complainant v Respondent.*[1656] This complaint was about the use of CCTV camera in residential areas. The complainant lodged it on 8 November 2010 by way of a letter to His Excellency, the President of Mauritius and to the Commissioner of Police. On 25 January 2011 the Commissioner of Police channelled the letter to the Data Protection Commissioner. The complainant alleged that his neighbour, who is the respondent, had placed CCTV cameras in his yard, the visual angle of which was directed towards him. As a result, it had caused and was continuing to cause heavy prejudice to him by violating his privacy. The complainant further alleged that because of the acts of the respondent he was not able to open his kitchen room and his family was suffering from intense heat during summertime.

Upon consent by the respondent, the Commissioner investigated the complaint. The site visit was carried out in the presence of both parties. The investigation revealed that the images which were recorded in the respondent's camera did not capture anything outside the respondent's site. Moreover the respondent justified the continued use of CCTV cameras for privacy and security

[1656] Ref.No:-PMO/DPO/DEC/2.

reasons. Following this investigation, the complainant gave a written declaration that the cameras placed by respondent were not infringing his privacy rights since they were not directed towards his premises and was satisfied with the enquiry carried by the Commissioner.

The Commissioner decided that there was no any incriminating evidence against the respondent. Nonetheless, she required the respondent to place within two months of the date of receipt of the decision, a small but visible and legible sign near his entrance gate or any other appropriate area within his premises to inform all visitors that CCTV cameras were in operation for security purposes. The rationale for this was to prevent any potential infringement of privacy rights of individuals and violations of sections 22, 23, 24, 25, 26, 27,28 and 29 of the DPA. The respondent was further required to notify the Commissioner the compliance to her direction failure of which would result into commission of an offence under section 12 of the DPA. The Commissioner set aside the complaint under section 11 of the DPA as the commission of an offence under the DPA had not been proved beyond reasonable doubt. This decision was delivered on 25 April 2011.

The above decision shows that the Commissioner did not specifically refer to the 'Guidelines to regulate the Processing of Personal Data by Video Surveillance Systems-Volume 5' although she applied some of the rules laid down there. Moreover, in contrast to the first decision, she set it aside under section 11 of the DPA.

The third decision is *Complainant v Respondents 1 and 2*.[1657] The complaint involved here was about unauthorised marketing by short service message (SMS). It was lodged on 17 December 2010 and was decided on 26 June 2011. In this matter it was alleged that the complainant received an SMS on his private mobile phone number reading as follows: 'INVEST IN LAND. Buy land on the heights of Les Marianes. Show day 19 December from 14h30 onwards. Phone (respondent 1) for more info :(...)' without his consent. The complainant's number was private and registered on his name at Orange Mauritius Telecom. He requested an enquiry by the Commissioner as to how the leakage of his private mobile number had taken place.

For investigation of the above complaint, the Commissioner delegated her powers to an investigative officer outside the Commission as the complainant was an officer of the Commission. The complainant voluntarily showed the SMS concerned with the advert to the

[1657] Ref.No:-DPO/DEC/3.

enquiring officer. The enquiry revealed that respondent 1 had outsourced the marketing activities of the company to respondent 2, a data processor. Respondent 1 further stated by way of declaration that he had been made aware of the relevant sections of the Data Protection Act namely sections 22, 24 and 30 and that he was satisfied with the enquiry conducted by the Commission.

Respondent 2 informed the Commissioner by way of a written statement that he had constituted a database of his customers which consisted of their demographic details and phone numbers. He also stated that the marketing activities of the company were carried out with prior consent of his customers through duly signed forms. Moreover, each month a customer was sent a message to deregister should he or she wish to do so. In event there was no reply, customers remained in the database. During the site visit, carried out with respondent 2's consent, the latter showed the enquiring officer the mobile number used to contact the customers monthly, consent forms, and those who declined their consent. Respondent 2 also stated that the incident comprising the complaint cropped up due to an inadvertent error wherein a number had been wrongly or erroneously inputted in the database or a subscriber failed to deregister from the service when given the opportunity. He further gave assurance that minute care would be exercised to prevent the recurrence of such incidents in the future and was satisfied with the manner the enquiry was conducted.

During investigation, the enquiring officer informed respondent 1, that in accordance with section 24 of the Data Protection Act, he must ensure that respondent 2 was only sending SMSs to those consented to receive the required advert. The enquiring officer required respondent 2 to stop sending SMSs though there was initially a written consent to accept SMSs about marketing when the customer did not wish to receive SMSs anymore. Respondent 1 was required to notify all its agents and concerned stakeholders to ensure that express consent of individuals for marketing had been obtained before any advert was sent through a third party or data processor to them. Moreover, the complainant gave a written declaration that he was satisfied with the outcome of the enquiry and the prompt action taken by the Commissioner. Since corrective measures had already been implemented by the respondents he had not received any more advert SMSs from them.

The Commissioner found that it was proved beyond reasonable doubt that the SMS complained was sent through a genuine error to complainant on his mobile and was not meant to cause any

prejudice to him. Nevertheless, she required both respondents to carry out direct marketing activities in compliance with the requirements of the DPA, particularly Part IV. She also required the respondent 1 to provide a more user friendly and efficient marketing system where the option to deregister or opt-out was incorporated in the SMS (containing advert) itself before sending. The Commissioner required respondent 1 to envisage opt-in consent to confirm express consent of the customers electronically together with the signing of the appropriate consent forms as already catered for by him. Respondent 1 was similarly required to comply with the principle of purpose specification and security. Respondent 2 was required under section 27 of the DPA to enter into a contract with the data processor, i.e. respondent 1, which stipulates that the latter would only act on instructions received from the data controller, i.e. respondent 2 and was bound by the obligations devolving on the data controller. The complaint was thus set aside to the above legal conditions being fulfilled.

As it can be noted, the Commissioner's above findings do not refer or in any case take into account the provisions of 'A Practical Guide for Data Controllers & Data Processor-Volume 1' regarding direct marketing. As a result, her decision is fundamentally inconsistent with her own guidelines. Particularly significant to note, the Commissioner has complicated the data subject's requirement of consent in the context of direct marketing. Whereas in the Practical Guide she was prepared to accept 'passive consent' i.e. failure by the data subject to 'tick a box' marked 'opt-out' in compliance with the provisions of the DPA, in the present decision she insisted on express consent standard. Moreover, the Commissioner's view, that the express consent already obtained by the respondent 1 in duly written forms was to be supplemented by an electronically 'opt-in' consent to confirm the previously obtained consent, was rising the standard too high. It can be argued that the two-stage consent approach may not be in compliance with section 24(1) of the DPA which imposes duty on data controllers and processors to obtain 'express consent' before processing personal data. This provision or section 30 of the DPA does not impose an extra duty to 'confirm consent' by obtaining another 'express consent' in respect of the same personal data and for the same purpose.

It is imperative to note that in the present case the Commissioner found sufficient evidence that respondent 1 used the complainant's private mobile phone number without his consent. Yet she was prepared to accept 'genuine error' as defence to mitigate the effect of the unlawful use of one's private mobile phone number. Nevertheless, it is difficult to comprehend where and how

respondent 1 picked the private mobile phone number of the complainant, perhaps due to the amount of details reported.

This complaint also demonstrates possibilities of conflicts of interest surrounding the functions and powers of the Commissioner. As allude to, the complainant in the present complaint was an officer working in the Data Protection Office. To partly resolve the conflict of interest, the Commissioner delegated her powers to investigate to another person. While this is commendable approach, it has to be noted that the same Commissioner proceeded to decide the complaint. It is not clear how she dealt with the issues of conflict of interest at the decision stage. It is submitted that merely working together with the Commissioner may not necessarily prevent the latter from deciding a complaint involving a co-employee.

The fourth complaint, *Complainant v Respondent,*[1658] is similar to the second in that they are both related to unauthorised use of CCTV cameras. The former was lodged on 13 April 2011 under section 11 of the DPA and its decision was passed on 5 August 2011. In this complaint, the complainant alleged that the respondent placed his CCTV cameras in such a position as to affect his private life through the monitoring of his movements from and to his dwelling house. He provided the schema of the alleged positioning of the camera systems where he resided.

On a site visit to the respondent's premise which was conducted with her own consent it was revealed that, the respondent installed the CCTV cameras to deter vandalism from students, trespassing of her pupils to neighbouring houses and littering on the school compound. She also gave concrete experiences leading to installation of the CCTV cameras. Despite the justification, the investigation revealed that two cameras slightly focused beyond the boundary walls because they were long range surveillance. As a result, passerby and vehicles could be viewed outside the college premise. The respondent confirmed to the enquiring officers that she had no malicious intention to invade the privacy rights of the complainant and/or neighbours. She installed the cameras systems for security purposes only. Moreover, she stated that immediate measures for compliance would be taken for reorienting all cameras to focus the premises of the college only. The respondent had already placed sign boards after the first site visit. However, the respondent failed to successfully take corrective measures. Following this failure, the Commissioner served the respondent with an enforcement notice which she complied with.

[1658] Ref.No:-DPO/DEC/4.

Based on the above, the Commissioner decided that the respondent had implemented corrective measures to safeguard privacy rights namely posting of proper signage to inform all the college's premises of the presence of CCTV cameras. That was in compliance with sections 22, 23, 24, 25, 26, 27, 28 and 29 and Part VI of the Data Protection Act. Moreover, the enforcement notice served to the respondent had been observed by her.

Like the second decision, the Commissioner properly applied some rules in the 'Guidelines to regulate the Processing of Personal Data by Video Surveillance Systems-Volume 5' without express reference to it. However in this particular complaint the Commissioner found sufficient evidence to incriminate the respondent yet she avoided to reach such a conclusion. Although not specifically stated, this may be partly due to the Commissioner's acceptance of the respondent's defence of 'no malicious intention to invade the privacy rights of the complainant and/or neighbours.' Instead, she said that the respondent had implemented corrective measures and complied with the enforcement notice. It is also important to note that this is the only complaint in which the Commissioner had used the enforcement notice to make the respondent compliant to the provisions of DPA.

The fifth decision, *Complainant v Respondent*,[1659] is about unauthorised marketing by phone. The complaint was lodged on 17 December 2010 under section of 11 of the DPA and decision was passed on 17 August 2011. The complainant alleged that he received a call from someone claiming to be calling on behalf of the respondent from telephone number (...). The person calling said to the complainant that he got complainant's number from Orange (a Telecom company in Mauritius). He also claimed that the complainant was very lucky to have won a 50% off discount on the training courses the respondent was offering. The complainant stated in his complaint that he had never played any game to receive that discount nor had he granted written authorisation to Orange to disclose his private phone number to any third party. Due to that, the complainant requested the Commissioner to investigate how the leakage of his private mobile number had taken place.

The Mauritius Telecom informed the Commissioner that the complainant's number (...) was not within the public domain and was registered as a prepaid SIM in their system. Also, it was not the policy of MT/Cellplus to disclose details of subscribers to third parties. MT was also neither in any business relationship or partnership with the respondent.

[1659] Ref.No:-DPO/DEC/5.

In the course of investigation, the enquiring officer contacted the respondent and informed him the implications of marketing by phone with emphasis on Part IV of the Data Protection Act. The enquiry had also revealed that the respondent was not aware of the provisions of the Data Protection Act.

By way of written declaration, the respondent confirmed that he was not in partnership with Orange/Emtel for marketing activities but did marketing to all customers of Emtel and Cellplus. The respondent stated that the mobile numbers of customers were chosen at random to contact them and the company does not phone customers anonymously. Upon calling, they introduced themselves first and then asked for permission before talking to the customer. If the person agreed, they then proceeded with their marketing; else they stopped the marketing procedure immediately. The respondent also stated that those customers who did not consent to take the call were recorded in a database and were not contacted further. Similarly, the respondent kept a database of phone/mobile numbers for those who expressly consented and were interested to take any course from the respondent. He showed the records in the database.

The enquiring officer informed the respondent a number of practical steps to comply with the provisions of the DPA in the marketing of his business: to establish a written contract for those customers who wanted to be contacted further with the option of 'opt-out' incorporated in the marketing agreement. Such agreements must be duly signed by the subscriber who accepted to receive any advert concerning ICT Training course from respondent. The respondent was also informed to contact only clients who had provided their written consent and stop immediately under the provision of section 30 of the DPA marketing for those customers who no longer accepted the marketing though they had initially signed consent forms to receive adverts. The enquiring officer also informed the respondent to adhere to section 22 of the DPA which is about purpose specification. The respondent was also informed to use other means of marketing as public broadcast media such as television, radio and/or written press. The enquiring officer insisted that marketing by phone could only be done with express consent.

The complainant gave a written declaration that he was satisfied by the investigation carried out by the Commissioner which remedied the matter. He also informed the enquiring officers that he had not received any call from the respondent after the complaint was lodged in the office of the Commissioner. Similarly, the respondent declared in writing that he was satisfied with the

enquiry carried out by the Commissioner and would ensure compliance to the provisions of the Act.

The Commissioner decided that it was proved beyond reasonable doubt that the call was made to the complainant on his mobile by the respondent. She required the respondent to carry out his marketing activities in compliance with the relevant provisions of the Data Protection Act particularly Part IV. Similarly the Commissioner required the respondent to provide a more user friendly and efficient marketing system whereby the option to deregister or opt-out is given whilst securing written consent of the customers for marketing. The consent collected should not be used for any other purpose incompatible with the original purpose. He was also required to ensure appropriate security and organisational measures are taken to protect the personal data of customers.

It can be noted from the above; the Commissioner required only 'express consent' as opposed to both 'express consent' and confirmation of the previous consent by 'opt-in' option in the third decision. The latter is practically new and/or additional 'express consent'. Therefore while the two complaints are slightly similar, the level of consent required has not been consistent. Moreover, contrary to the Practical Guide where it is provided by the Commissioner that express consent may be oral or written, in the present decision she insisted that written consent must always be given. Also important to note, although the Commissioner found the respondent incriminated by evidence, she did not say so expressly. Instead, she proceeded to direct corrective measures. Lack of awareness or rather ignorance of the law pleaded by the respondent might have influenced the Commissioner not to strictly deal with the respondent. However such defence raised by the respondent had not been expressly considered. The other point which is difficult to comprehend is the respondent's approach of choosing randomly customers of Orange and Emtel. Although both, the respondent and MT/Cellplus denied to have any relationship, one is made to believe that such relationship might have existed otherwise the respondent could have nowhere to pick customers' mobile phone numbers in the first place.

The sixth decision is *Complainant v Respondent.*[1660] It was about unauthorised use of private e-mails. The complainant was lodged on 18 February 2011 by way of letter and decided on 26 August 2011. The letter was from anonymous data subjects. Their claim was that the respondent had emailed symbolic pictures of a religious nature to several persons. He used email addresses of

[1660] Ref.No:-DPO/DEC/6.

complainants without their authorisation. The complainants alleged that the respondent used their email addresses allocated to them by the organisations they were working for as such he divulged their private addresses and infringed their right of privacy.

The Commissioner investigated the complaint submitted to her under the powers vested in section 5(f) of the DPA. Under this provision the Commissioner may initiate investigation on the basis of suspicion received by her that an offence under the Act may be committed. In the present complaint the complainants were anonymous. Hence the complaint letter sent to her was sufficient to trigger intervention of the Commissioner even if the complainants remained anonymous.

By way of a written declaration, the respondent confirmed to have sent the email in question from his employee mailbox to various recipients. However, he stated that he did so without malicious intention to harm anybody since he did it according to his religious beliefs and as a well-wisher. He further stated that, in his opinion, some people or one of the email receivers were attempting to put his professional career at stake by making an anonymous complaint. The respondent also stated that he would cooperate fully with the Commission in its investigation. In another statement, the respondent stated that he had been made aware of the relevant provisions of the Data Protection Act with regard to the complaint made against him. He was satisfied with the way the enquiry was conducted.

The Commissioner decided that it was proved beyond reasonable doubt that the respondent was not aware of implications of sending email addresses of third parties to unauthorised recipients and there was no mala fides involved in his action. The enquiring officers informed him such implications. The Commissioner reminded the respondent that under section 24 of the Data Protection Act of his duty to obtain the express consent of a data subject before using the latter's personal data. She also informed the respondent that failure to abide by the provisions of the Act would result in prosecution by the Commission.

This decision is the first in which the Commissioner expressly accepted lack of awareness of the provisions of the Data Protection Act (i.e. ignorance of law) as a defence for unlawful processing of personal data. She similarly accepted lack of malicious intention to harm anybody as a defence.

The seventh complaint is *Complaint v Respondents 1 and 2*.[1661] The complaint in his decision concerned about the use of personal data in the context of debit/credit card. It was lodged on 7 June 2011 and decided on 14 May 2012. Initially, this complaint was lodged on 3 March 2011 by letter to the General Manager of respondent 1 and the CEO of respondent 2. The copy of the complaint was sent to the Prime Minister's Office (Defence and Home Affairs Department). It was subsequently channelled to the Commissioner. The complainant alleged that respondents 1 and 2 stored his debit/credit card details during purchase transaction at Point of Sale (POS). During investigation-the complainant showed the investigators his debit card he used to pay at the POS as well as a copy of respondents' 1 and 2 receipts where the debit/credit card number was recorded. The complainant alledged that his details could be used for illicit payment by hackers. Moreover, the Commissioner requested necessary advice from two unnamed sources. The Commissioner decided that it was proved beyond reasonable doubt that respondents 1 and 2 displayed the required efforts to remedy the potential dangers to personal information of customers being used for illegal transactions by adopting appropriate security and organisational measures. However, the Commissioner required the respondents to show compliance with international and local standards by ensuring that personal information as identified above are not kept illegally.

An overview of the above decisions reveals the following common trends. First, in all complaints the standard of proof is beyond reasonable doubt. However, it is less clear who primarily bears the burden of proof. In some cases, the burden lays upon complainants yet in certain other cases upon the respondents. Also less obvious is the criterion for the shift of this burden. Second, somewhat related to the first, the Commissioner has not strictly enforced the provisions of the DPA and its regulations. In most cases where she found controllers contravened the law, the Commissioner avoided to find so expressly. Instead, she proceeded to give corrective measures. This is partly because many data controllers and processors in Mauritius are not aware of their obligations, suggesting why the Commissioner has accepted ignorance of law and/or lack of awareness of the provisions of the DPA as a defence. As a result, the Commissioner has utilised the proceedings arising out of the complaints lodged in her office to bring the provisions of the DPA and its regulations in the knowledge of the data controllers and processors. To accomplish that mission, the enquiring officers spend substantial part of the investigation to explain to the data controllers and processors their obligations under the Act. Similarly, the Commissioner makes reference to various provisions of the Data Protection Act in her decisions even if they

[1661] Ref.No:-DPO/DEC/7.

are not directly applicable to a particular dispute. Third, there are no formal definitions of complaint outcomes. For example, in the first three decisions the Commissioner used the expression 'set aside' while in the seventh case no express outcome is declared. Yet, in setting aside the first decision, she did so under sections 26(a) & (b) and 28 of the DPA while in the second and third decisions she set aside the complaints under section 11. Surely, the Commissioner erred to set aside the first decision under the substantive provisions rather than section 11 of the DPA. Yet 'set aside' is not clear as sometimes it appears to mean the complaint is not founded hence dismissed as it was the case with the second complaint. However, 'set aside' appears also to mean the complaint has been resolved as in the third complaint. On the other hand, the Commissioner has not used the term 'set aside' in the fourth, fifth, sixth and seventh decisions. Hence, it is difficult to ascertain readily the outcomes of such complaints. It is submitted that, consistency in reporting outcomes of complaints is necessary. The latter is also required to be made around formalised definitions which explain the meaning of complaint outcomes, e.g. resolved, settled, dismissed, withdrawn, etc. Fourth, the current way of anonymising parties to the complainant is somewhat confusing. As alluded to, parties are called as 'complainant(s)' and 'respondent(s)'.For example the parties in the second, fourth, fifth and sixth appear to be the same. This may cause difficulties to properly distinguish these decisions. An alternative way of achieving anonymity, while maintaining degree for distinguishing decisions is to refer to the names of parties with their initial capital letters of their first names (e.g. Z v P). Also important in citation of decisions is to add years of decisions. This may help to obtain the statistics of the complaints in a particular year. Fifth, in all seven decisions, the Commissioner has not explained to the parties their right of appeal to the ICT Appeal Tribunal as is required under section 11(b) of the DPA. It is not certain whether the Commissioner has been using a different method to notify the parties of this right. During interview with the researcher of this thesis on 4 July 2011, in Port Luis, Mauritius, the Commissioner confirmed that none of the first three decided decisions by then was appealed to the ICT Appeal Tribunal partly because parties were satisfied by the Commissioner's decision. However, one point has to be made clear. None of the above seven decisions ended with a consent settlement of parties. Hence the signed declarations by parties in the Commissioner's decisions that they were satisfied with the way the complaint and/or investigation were handled do not qualify as settlement to bar appeals. It is imperative to note that the Commission's website is not linked to the website of the ICT Appeal Tribunal. This partly makes difficult to ascertain if there is any appeal in the Tribunal arising from the Commissioner's decision. Also significant to note is that there is no known case law in which a data subject has instituted in the ordinary courts for compensatory claims. Finally, it can

be submitted that most of the problems enumerated above are largely caused by absence of regulations on proceedings of the Commission in determining complaints. In connection with this, the Commissioner once observed that section 11 of the DPA simply provides for investigation of the complaint, notification to the complainant in writing of her decision and information about the appeal to the ICT Appeal Tribunal.[1662] 'There is no provision in the Data Protection Act on the manner in which a hearing may take place and the evidences(sic) to be submitted before the Commissioner...'[1663]

- **Annual Reports**

Section 55 of the Data Protection Act requires the Commissioner to lay an annual report to the National Assembly. The Commissioner has to table the report three months latest after the end of the calendar year. Section 55(3) provides that the first calendar year covered the period from the commencement of the DPA to the end of the year of such commencement. Since the rest of the DPA came into force on 16 February 2009, the latter was the commencement of the first year of the report while 31 December 2009 was the last date. Accordingly, the Commissioner had up to 31 March 2010 to lay her first annual report to the National Assembly. In compliance to the time limit, the Commissioner has so far laid her first annual report (February 2009-Decemnber 2009), second annual reports (January 2010-December 2010) and third annual report (January 2011-December 2011).

The contents of the Commissioner's reports are largely determined by herself. However section 55(2) states that the annual report shall include a statement about the operation of approved and issued codes of practice and any recommendation relating to the compliance with the Act, and in particular the data protection principles. All of the Commissioner's three reports contain the minimum contents required by the law. Other issues included in the reports are registration of data controllers and processors; sensitisation; complaints; investigations; and threats to data protection generally. Some shortcomings of these reports are: they lack special formats as a result it is difficult to follow the progress of particular issues. For instance, the first report states the vision and mission of the Data Protection Office while the second states only the vision yet with slight difference from the first. Also, the reports do not cover decisions of the Commissioner

[1662] Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009-February 2010, p.14.
[1663] Ibid.

regarding complaints submitted in her officer. Apart from being posted on the Commission's website it is not certain if these reports are disseminated to data controllers and processors.

5.4.3 EU-Accreditation Process

This part comprises of an extended discussion of part 5.4.2.2 dealing with legislative process. It has been dealt separately for three reasons. First, is to give clear focus of discussion of the issues falling under accreditation stage. Second, there is no clear evidence of the direct involvement of the European Union in the legislative process already covered in 5.4.2.2. As discussed elsewhere in this thesis, this second reason stems out of the fact that it is the third country which initiates the accreditation process and not EU itself. Third, during accreditation stage, the European Union is largely involved to streamline the third country's data legislation already in place. However two caveats must not be forgotten. Most invariably the legislative process in a third country (e.g. part 5.4.2.2) is initially influenced and driven by the objective of adopting the data privacy law in line with the requirements of Arts 25 and 26 of Directive 95/46/EC. Moreover, quite often such a legislative process involves copycat of the basic principles and provisions of the Directive 95/46/EC and institutions of enforcement. Sometimes a third country takes a statute on data privacy from an EU member state which had already transposed the Directive. Therefore while the accreditation process is a component of legislative process it deserves its own treatment.

As pointed out, the Mauritius Data Protection Act 2004 was adopted largely to secure the business agenda. Not surprisingly compliance with the European Directive 95/46/EC was/is necessary to ensure uninterrupted flow of personal data from Europe to Mauritius. In the first annual report to the National Assembly, the Data Protection Commissioner reported:-

> 'The prime objective of the Commissioner in 2009 has been to pave the way to the international recognition of the office through accreditation of Mauritius with the European Union. A project becoming reality since the European Union has officially been requested to consider extending to Mauritius the status of an adequate third country in data protection and the issue is presently being considered at the level of the EU.'[1664]

[1664] Ibid, p.1.

The Commissioner also reported to the National Assembly that in response to the above official request for accreditation, a consultant (representing University of Namur) appointed by the European Union went to Mauritius in March 2010 to study the Data Protection Act and the level of compliance of the Mauritius data privacy legislation with European standards.[1665] The report of the consultant would then be forwarded to the European Union who would make proposals with regard to any amendments to be brought to the Data Protection Act to satisfy the safeguards provided under the European Direction on data protection.[1666]

In 2010 the European Union issued its report on the adequacy level of data protection afforded by Mauritius.[1667] This report did not clear Mauritius as providing adequate level of protection of personal data as the Commissioner states:-

> 'The office has since its inception been working on the adequacy procedure and in 2010 a first report of the EU demonstrating the required improvements to be made to the legislation was finalised. The office has drafted the required changes and is waiting the visit of a second EU consultant next week for the draft amendment bill to be finalised and presented to the National Assembly as soon as possible. Once the amendments made, the EU would have to consider the adequacy of Mauritius.'[1668]

As noted, Gayrel was one of the European Union consultants who evaluated the data protection law in Mauritius. Her article titled 'Mauritius: Data protection in an evolving island economy' has substantially highlighted the deficiencies of the Mauritius data protection system based on the adequacy report.[1669] Because of this, no detailed discussion of the report is offered here.

On 24 November 2011, the 'Workshop for the Mauritius data protection accreditation with the European Union' was held in Port Louis, Mauritius. It was facilitated by the second consultant for the European Union, Mrs. Tira Greene. The workshop was also attended by the Ambassador of the European Union in Mauritius, Hon. Alessandro Mariani. Other participants included the

---

[1665] Ibid, p.4.
[1666] Ibid.
[1667] CRID, University of Namur (Belgium)., 'Analysis of the adequacy of protection of personal data provided in Mauritius: draft final report, 2010.
[1668] Madhub, note 1566, supra.
[1669] Gayrel, note 1334, supra.

Minister of Information and Communication Technology, Mr. Pillay Chedumbrum, Attorney General, Hon. Yatin Verma and Mrs. Madhub, Data Protection Commissioner.

Mr. Mariani said the workshop was held in the context of the technical assistance being provided by the European Union to the Prime Minister's Office and to the Data Protection Office.[1670] He further pointed out that the objective of the consultancy was to pave the way for the compliance of the data protection legislation in Mauritius with European Union's standard.[1671] Emphasising the economic agenda for the compliance, Mr. Mariani posited that it was of utmost importance that the data protection legislation and principles in Mauritius was made compliant with the European Union Directive.[1672] That would secure better chances that Mauritius was recognised by the European Union as a country where data protection is adequate, thus opening up opportunities for Foreign Direct Investments in important sectors such as offshore and business processing outsourcing.[1673]

On the other hand, the consultant, Tira Greene, pointed out a number of areas which required amendments. These included certain definitions of the Data Protection Act to be amended to correspond to those in the Directive, particularly definitions of personal data, processing, individual; provision on processing of sensitive personal data, transfer of personal data and exemptions to be amended to correspond to those in the Directive; removal of the requirement for renewal of registration; section 51 of the DPA on 'information available to the public' was not compliant to the Directive hence it was required to be repealed; the right to object to be inserted and some e-government provisions.[1674]

It is submitted that although the Data Protection Act in Mauritius was adopted in order to offer individuals protection of their privacy and to facilitate transfer of personal information in the context of business, the latter appears to be the broad agenda for accreditation. Since the transfer of personal information envisaged in the accreditation relates to individual residents or citizens of EU countries, it is the effect of Mauritius Data Protection regime over the latter that counts

[1670] Speech of H.E Mr. Alessandro Mariani, Ambassador of the European Union in Mauritius during 'Workshop for the Mauritius Data Protection Accreditation with the European Union,' Domaine Les Pailles, 24 November 2011, p.1, http://www.gov.mu/portal/goc/dpo/files/EU_Ambassador.pdf last visited 4/04/2012.
[1671] Ibid.
[1672] Ibid, p.3.
[1673] Ibid.
[1674] Greene, T., 'Data Protection Accreditation for Mauritius' Port Louis, Mauritius, 24 November 2011, http://www.gov.mu/portal/goc/dpo/files/pres_eu1.pdf last visited 4/04/2012.

towards adequacy hence accreditation rather than the effect produced by the same regime on its own citizens.[1675]

5.4.4 Other Legislation

The most important of other pieces of legislation regulating protection of personal data is the Information and Communication Technologies Act 2001.[1676] Previously this Act incorporated the regime of data protection law in section 33 and the Fourth Schedule. The latter detailed the data protection principles somewhat similar to the First Schedule of the Data Protection Act 2004. However the entire regime of data protection in the ICT Act 2001 was repealed by section 64(2) of the Data Protection Act 2004. Currently the ICT Act regulates matters of interception of communication under section 32(3) based on limited provisions of confidentiality.

The next statute is the National Computer Board Act 1988.[1677] Like the ICT Act, the entire regime of data protection in the NCB Act 1988 has been repealed by section 64(3) of the Data Protection Act 2004. This is also the case with Criminal Code Cap 195. Previously, the Criminal Code contained a regime of data protection in section 300A. The later has been repealed by section 64(1) of the Data Protection Act 2004.

Other pieces of legislation with remote regimes of data protection are the Computer Misuse and Cybercrime Act 2003[1678] and Electronic Transactions Act 2000.[1679] The former statute applies in the context of criminal activities perpetrated through computer systems while the latter applies in the electronic transactions and communications. Issues under this legislation include e-commerce, liability of service providers, electronic and digital signatures, etc. Both the Computer Misuse and Cybercrime Act 2003 and Electronic Transactions Act 2000 have never been affected by the Data Protection Act 2004. The reason is that they are not directly related with regulation of personal data.

[1675] For similar view, see e.g. Greenleaf and Bygrave, note 905, supra.
[1676] Act No. 44 of 2001.
[1677] Act No.43 of 1988.
[1678] Act No. 22 of 2003.
[1679] Act No.23 of 2000.

5.5 Conclusion

This chapter has shown that privacy is still an evolving concept in Mauritius. The development of the ICT sector has largely attributed to the rising concerns for individuals' privacy. However, lack of awareness rather than collectivism affects the culture of data protection for majority of Mauritians. Moreover the endeavours by the Mauritius government to develop and promote the ICT sector to become the fifth pillar of the country's economy serve as the broad agenda for the adoption of the data protection regime. The key players in the ICT sector are foreign companies largely originating from Europe. As a result the European Union is keen to ensure that transfer of personal data in Mauritius must receive an adequate level of protection. At the same time Mauritius is putting efforts to streamline its data protection regime to comply with the European standards through the accreditation procedure. For Mauritius, compliance to EU standards is lucrative business as the latter will be able to engage in foreign direct investment in Mauritius, particularly in offshore and business processing outsourcing, without interruption.

6. Data Protection in South Africa

6.1 Introduction

South Africa has no comprehensive data protection legislation. However she has currently a data privacy protection Bill pending before the Portfolio Committee on Justice and Constitutional Development of the South African Parliament. This Bill is a product of the longest debates, public consultations and reports in the history of the country and Africa. The present chapter sketches the legislative development of the South African data privacy Bill alongside the socio-economic and political history of the country. In the course of these analyses, contested interests operating for and against the adoption of the data protection legislation are identified. Besides the Bill, this chapter offers an outline of the present systems of data privacy protection in South Africa. The strength and weakness of this system is provided as one of the justifications for adopting the omnibus data privacy law in the Republic.

6.2 Socio-Economic and Political Context

In contrast to many African countries, South Africa has a complex socio-economic and political history. Its thorough presentation deserves a separate treatment for want of space and time. This part provides only a summary of selected areas which are relevant to the theme of this thesis. The rest of the history is left out.

The Republic of South Africa (South Africa) is located in southern Africa, at the southern tip of the African continent. It extends 1,821 kilometres north east to south west of Africa and 1,066 kilometres south east to north west. South Africa's total area is 1, 219, 912 square kilometres. To the north, it is neighboured by Botswana and Zimbabwe; to the north east by Mozambique and Swaziland; on the east by the Indian Ocean; on the south by the Indian and Atlantic Oceans; on the west by the Atlantic Ocean; and on the north west by Namibia. In total South Africa is administratively divided into nine provinces: Eastern Cape, Free State, Gauteng, KwaZulu-Natal, Mpumalanga, Northern Cape, Limpopo, North West and Western Cape.[1680] The Capital City of South Africa is Pretoria. South Africa has also control of two small islands of Prince Edward and Marion which lie some 1,920 kilometres south east of Cape Town.

[1680] The Constitution of South Africa 1996, Art 103(1).

Demographically, South Africa's total population is estimated at 50.59 million.[1681] The main racial groups out of this population are Africans (79.5%), Coloured i.e. mixed-race descendants of early white settlers and indigenous people (9%), Indian/Asian (2.5%) and White (9%).[1682] According to the World Bank statistics, by 2010 more people in South Africa lived in the urban areas than in rural: in the former it was 60.7% and the latter 39.3%.[1683] There are 11 official languages in South Africa: Afrikaans, English, Ndebele, Pedi, Sotho, Swazi, Tsonga, Tswana, Venda, Zulu, and Xhosa.[1684] Each of them has an equal status as the other.[1685] Yet in practice English enjoys a relatively dominant position. Other languages such as German, Greek, Gujarati, Hindi, Portuguese, Tamil, Telegu, Urdu, Arabic, Hebrew, and Sanskrit are protected and promoted by the South African Constitution 1996.[1686]

South Africa is a secular state. However there are four dominant religions practiced by South Africans. These include Christianity 68 %(mostly Whites and Coloured, about 60% of blacks and about 40% of Indians); Islam 2%; Hindu 1.5 %(60% of Indians); indigenous beliefs and animist 28.5%.[1687]

Politically, South Africa is a multi-party constitutional democracy with the president as both head of state and government.[1688] At the provincial and local government level, the executive function is vested in the premier and municipal council respectively.[1689] The Constitution is the supreme law in the country.[1690] Any other law or conduct inconsistent with it is invalid.[1691] Democratically, South Africa is characterised as flawed democracy similar to Botswana, Cape Verde, Namibia, Lesotho, Benin, Mali, Ghana, and Zambia.[1692]

[1681] Statistics of South Africa, Mid-Year Population Estimates, 2011, http://www.statssa.gov.za/publications/P0302/P03022011.pdf last visited 6/04/2012. It is important to point out that the latest population census in South Africa was carried out in 2011, however the report has not yet been released.
[1682] Ibid.
[1683] World Bank Indicators, http://www.tradingeconomics.com/south-africa/population-density-people-per-sq-km-wb-data.html last visited 6/04/2012.
[1684] The Constitution of South Africa 1996, Art 6(1).
[1685] Ibid, Art 6(4).
[1686] Ibid, Art 6(5).
[1687] South African Web, http://www.saweb.co.za/provs.html last visited 6/04/2012.
[1688] The Constitution of South Africa 1996, Arts 1 and 83.
[1689] Ibid, Arts 125(1) and 151(1).
[1690] Ibid, Art 2.
[1691] Ibid.
[1692] The Economist Intelligence Unit, note 1510, supra. Note that Mali, Zambia and Ghana have been changing their status in 2007, 2008, 2010 and 2011 reports.

South Africa became independent from the British colonial rule on 31 May 1910. However it remained under the white minority rule until 27 April 1994 when she attained majority rule. This date is the South Africa's Freedom Day and officially the Independence Day. Prior to the South Africa's Freedom Day, the country had experienced the Dutch and English colonial rule just as it was the case with many African countries. However, this was compounded by the worst form of racism and apartheid regime which was officially launched in 1948, the date when the National Party (NP) came in power, and ended in 1994.[1693]

Apartheid was a system of racial segregation enforced through legislation by the National Party governments of South Africa between 1948 and 1994.[1694] During this period, the rights of the majority non-white inhabitants of South Africa were curtailed and white supremacy and Afrikaner minority rule was maintained.[1695] Welsh posits that one of apartheid's chief aims was the elimination of competition between black and white, invariably to the benefit of whites.[1696] In significant respects the linchpin of the apartheid system was the Population Registration Act 1950, which in principle sought to classify every South African according to 'race'.[1697] As cruel in its consequences, though for many people, the Group Areas Act 1950 was another fundamental pillar of apartheid.[1698] It subsumed all previous pieces of legislation, notably the *ad hoc* attempts of previous governments to curb the so-called Indian 'penetration', by providing for the comprehensive residential and business segregation of the different colour groups in every city, town and village.[1699] Other pieces of legislation that consolidated apartheid system included the Bantu Building Workers Act 1951 which permitted Africans to perform skilled building work in the African townships, at lower wage rates than their white counterparts, but prohibited them from doing so outside African areas.[1700] A far-reaching in its scope, was the introduction of 'job reservation' in terms of an amendment to the Industrial Coalition Act 1956.[1701] This Act empowered the Minister of Labour to reserve particular categories of work for a specific racial category.[1702] The Promotion of Bantu Self-Government Act 1959 was yet another important

[1693] See e.g., Welsh, D., The Rise and Fall of Apartheid, Jonathan Ball Publishers, Johannesburg/Cape Town, 2009, particularly Chapter 3; Cottrell, R.C., South Africa: A State of Apartheid, Chelsea House Publishers, Philadelphia-U.S.A, 2005.
[1694] Wikipedia., 'Apartheid in South Africa', http://en.wikipedia.org/wiki/Apartheid_in_South_Africa last visited 6/04/2012.
[1695] Ibid.
[1696] Welsh, p.56, note 1692, supra.
[1697] Ibid, p.54.
[1698] Ibid, p.55.
[1699] Ibid.
[1700] Ibid, p.57.
[1701] Ibid.
[1702] Ibid.

piece of legislation. Through this Act, the so-called 'Bantustans' which means separate and supposedly autonomous black African states were established.[1703] Africans were required under this law to live in the Bantustans but nowhere else. There was also the Prohibition of Mixed Marriage Act 1949 which prohibited by deeming null and void marriages between white people and people of other races.[1704] A series of other pieces of legislation were also enacted in the fields of education, health and medical care, voting, access to public services, recreation, etc.

A point has to be made that, although apartheid officially commenced in 1948, its foundation was laid down since the early Dutch settlement in South Africa. Historians narrate that it was in 1652 when the Dutch through the Dutch East India Company, led by Jan van Riebeeck decided to establish permanent settlement at Table Bay.[1705] The primary reason for establishment of this settlement was to provide Dutch ships and other Europeans on their way to East Indies with foodstuffs and refreshments.[1706] The Dutch settlement and gradual expansion into the interior of South Africa resulted in clashes with the original inhabitants-the Khoisans.[1707] In 1795 when the Dutch influence was fading, the British took over the control over South Africa to prevent it from falling in the hands of the French.[1708] It is imperative to mention that some of the historical events which resulted in and/or accentuated the apartheid regime in South Africa were the Great Boer Trek (1830s-1840s),[1709] *Mfecane* Wars(1820s-1830s),[1710] the First (1880-1881) and Second (1899-1902) Anglo-Boer Wars,[1711] and the Union of South Africa of 1910.[1712]

[1703] Cottrell, p.92, note 1693, supra.
[1704] Ibid, p.102.
[1705] Ibid, p. 14.
[1706] Ibid.
[1707] Ibid.
[1708] Wikipedia., 'History of South Africa', http://en.wikipedia.org/wiki/History_of_South_Africa, last visited 7/04/2012.
[1709] The Great Trek (Afrikaans: Die Groot Trek) was an eastward and north-eastward migration away from British control in the Cape Colony during the 1830s and 1840s by Boers (Dutch/Afrikaans for 'farmers'). The migrants were descended from settlers from western mainland Europe, most notably from the Netherlands, northwest Germany and French Huguenots. The Great Trek itself led to the founding of numerous Boer republics, the Natalia Republic, the Orange Free State Republic and the Transvaal being the most notable, see Wikipedia., 'Great Trek', http://en.wikipedia.org/wiki/Great_Trek last visited 7/04/2012.
[1710] These wars were a result of the expansion of the European colonial settlement and trade in South Africa. They were other reasons such as scarcity of lands, etc. For detailed analyses of *Mfecane* Wars see e.g., Richner, J.E., 'The Historiographical Development of the Concept "mfecane" and the Writing of Early Southern African History, from 1820s to 1920s', M.A Thesis, Rhodes University, 2005.
[1711] These wars were fought between the British and the two Boer independent republics of Orange Free State and Transvaal Republic. The wars were part of the British effort to create the Union of South Africa for easy of control and administration.
[1712] The Union of South Africa came about on 31 May 1910 after unification of Cape, Natal, Transvaal and Orange Free State into the rest of South Africa under the British colonial control. The Union came to an end on 31 May 1961, when the country became Republic, see Wikipedia., 'Union of South Africa', http://en.wikipedia.org/wiki/Union_of_South_Africa last visited 7/04/2012.

The apartheid system left non-whites, particularly Africans with only one option of resisting it through militant and armed struggles. Some leading events which sparked and magnified the growth of African resistance were the Sharpeville Massacre of 21 March 1961, Soweto Uprising 1976-1977, restrictions of non-white movements such as the African National Congress (ANC) which operated through its armed wing, *Umkhonto we Sizwe* (Spear of the Nation), detentions and killings of leaders of African movement.[1713] Also significant to note is the fact that the opposition to apartheid arose outside South Africa notably from: United Nations, United States of America, Russia, United Kingdom, other European countries as well as African countries. Pressure on South Africa to abandon apartheid system from outside took largely the form of political and economic sanctions.

South Africa has a bicameral legislative system with the National Assembly as a lower house and National Council of Provinces as the upper house.[1714] The National Assembly is composed of not fewer than 350 and not more than 400 elected representatives.[1715] On the other hand the National Council of Provinces is composed of a single delegation from each province consisting of ten delegates.[1716] At provincial and local government levels, legislative functions are performed by the provincial legislatures and municipal council respectively.[1717]

The judicial authority in South Africa is vested in courts.[1718] The Constitutional Court is at the top in the hierarchy. It has jurisdiction to determine questions with regard to constitutions.[1719] Just below the Constitutional Court there is the Supreme Court of Appeal. The latter has jurisdiction to determine all appeals except in constitutional matters.[1720] The High Court is the third in judicial hierarchy. It has jurisdiction to determine any constitutional matter except those reserved for the Constitutional Court.[1721] Moreover, the High Court is vested with powers to decide any matter as assigned by an Act of parliament.[1722] Below the High Court, there are Magistrates' Courts and other courts with limited jurisdiction.[1723] These courts do not determine constitutional matters.[1724] It is important to note that the South African judiciary operates on a

[1713] See e.g., Welsh, Chapters 4, 5, 7 and 8, note 1693, supra.
[1714] The Constitution of South Africa 1996, Art 42.
[1715] Ibid, Art 46.
[1716] Ibid, Art 60.
[1717] Ibid, Arts 104 and 151(2).
[1718] Ibid, art 165(1).
[1719] Ibid, Art 167.
[1720] Ibid, Art 168.
[1721] Ibid, Art 169.
[1722] Ibid.
[1723] Ibid, Art 170.
[1724] Ibid.

hybrid of legal system. Due to the external influence as alluded to, South African legal system is largely made of Roman, Dutch and English law.[1725] As a result it is characterised by civil and common law traditions. Indigenous system of law also forms part of South Africa's legal system.[1726]

South Africa's economy has transformed significantly since the attainment of majority rule. Prior to that and more particularly during the apartheid era, the country's economy suffered stagnation and international isolation. Trade and financial sanctions and withdraw of significant of foreign investment in order to pressurerise South Africa to end apartheid regime had far reaching impact on the country's economy.[1727] There was yet another blow upon South Africa's economy. This was generated by the world economic conditions of the late 1970s and the early 1980s. As it was the case elsewhere in Africa, South Africa's economy slowed due to a number of reasons: the declining gold revenues, rising prices for oil imports and increased international competition in other traditional export commodities.[1728] By 1985 South Africa was hit by a major foreign debt crisis.[1729]

In its bid to reconstruct the country in the post apartheid era, the African National Congress (ANC), the ruling party led by Nelson Mandela(the first President after majority rule), embarked upon Reconstruction and Development Programme (RDP). The RDP included privatisation of parastatals, launching of worldwide appeals for new trade and investment packages, re-entering world financial markets, establishing new trade partners and expanding formerly clandestine trade ties that had long existed with many countries.[1730] As a result of these reconstruction efforts and despite the turbulence of economic crises in recent times, South Africa has successfully raised its economy. The country is now characterised by the World Bank as an upper-middle income economy.[1731] It is important to mention that South Africa's economy is reasonably

---

[1725] See e.g., Hahlo, H.R and Kahn, E., The South African Legal System and Its Background, Juta, Cape Town, 1968; Mireku, O., 'Three Most Important Features of South African Legal System that Others Should Understand', pp.215-217; IALS Conference, Learning from Each Other: Enriching the Law School Curriculum in an Interrelated World, http://www.ialsnet.org/meetings/enriching/mireku.pdf last visited 7/04/2012.
[1726] See e.g., Church, J., 'The Place of Indigenous Law in a Mixed Legal System and a Society in Transformation: A South African Experience', ANZLH E-Journal, 2005, pp.94-106.
[1727] Levy, P.I., 'Sanctions on South Africa: What Did They Do', Discussion Paper, No. 796, Yale University, 1999, pp.1-13, at p. 2, http://aida.wss.yale.edu/growth_pdf/cdp796.pdf last visited 7/04/2012.
[1728] South Africa-Economy,
http://www.mongabay.com/reference/country_studies/south-africa/ECONOMY.html last visited 7/04/2012.
[1729] Ibid.
[1730] Byrnes, R.M(ed)., South Africa: A Country Study, GPO for the Library of Congress, Washington, 1996, http://countrystudies.us/south-africa/61.htm last visited 7/04/2012.
[1731] World Bank List of Economies(July 2010), http://www.fas.usda.gov/mos/em-markets/World%20Bank.pdf, last visited 7/04/2012; see also, World Bank List of Economies(18 July 2011),

diversified with key economic sectors including mining, agriculture and fishery, vehicle manufacturing and assembly, food-processing, clothing and textiles, telecommunication, energy, financial and business services, real estate, tourism, transportation, wholesale and retail trade.[1732] The hosting of the 2010 FIFA World Cup has acted as a catalyst for expanding the country's infrastructure base, skills development, employment creation and economic growth.[1733]

In the field of international trade, trade relations with Europe, particularly with the European Union (EU), are pivotal to South Africa's economic development.[1734] It is imperative to note that the Trade, Development and Cooperation Agreement (TDCA) with the EU forms a substantial element of South Africa's reconstruction and development.[1735] Overall, the EU accounts for over 40% of South Africa's imports and exports, as well as 70% of foreign direct investment.[1736] Similarly South Africa is the largest EU's trading partner in Africa.[1737] To be sure, some EU member states such as the United Kingdom (UK), Germany, the Netherlands and Switzerland are among South Africa's top-10 export destinations.[1738] Germany, UK and France are among the top-10 countries from which South Africa's imports originate.[1739]

ICT is also an important sector in the South Africa's economy. The market for mobile phone is dominated by operators such as Vodacom, MTN, 8ta and CellC. By 2012 the total number of mobile phone subscribed is expected to reach 127%.[1740] In December 2011 there were 6,800,000 internet users in South Africa (representing 13.9% of the population).[1741] While it is difficult to provide concrete estimates of revenues collected from the ICT sector for lack of information, it is imperative to note that ICT is integrated in other sectors of the South Africa's economy. This integration facilitates the growth and development of such other sectors of the economy.

---

http://shop.ifrs.org/files/CLASS.pdf last visited 7/04/2012.

[1732] Wikipedia., 'Economy of South Africa', http://en.wikipedia.org/wiki/Economy_of_South_Africa last visited 7/04/2012.

[1733] Pocket Guide to South Africa 2010/11 Economy, pp. 48-58, at p.48, http://www.gcis.gov.za/resource_centre/sa_info/pocketguide/2010/008_economy.pdf last visited 8/04/2012.

[1734] Ibid, p.54.

[1735] Ibid.

[1736] Cooperation Between the European Union and South Africa: Joint Country Strategy Paper 2007-2013, p.12, http://ec.europa.eu/development/icenter/repository/print_csp07_za_en.pdf last visited 8/04/2012.

[1737] Ibid.

[1738] Pocket Guide to South Africa 2010/11 Economy, note 1734, supra.

[1739] Ibid.

[1740] South Africa-Telecoms, Mobile, Broadband and Forecasts, http://www.budde.com.au/Research/South-Africa-Telecoms-Mobile-Broadband-and-Forecasts.html last visited 8/04/2012.

[1741] Internet Worlds Stats., 'Internet Usage Statistics for Africa', http://www.internetworldstats.com/stats1.htm last visited 8/04/2012.

Socially, the South African society is both individualistic and collectivist.[1742] Professor Geert Hofstede indicates that South Africa has high index score of 65 for individualism measured in values range from 0 to 100.[1743] One reason this score is much higher than that of most African nations is the high level of European influence in the country.[1744] In contrast, black individuals from the Xhosa, Zulu and Sotho tribes tend to have much lower individualism indexes.[1745] As alluded to, the latter has been frequently explained by commentators as due to *Ubuntu*. The value of *Ubuntu* has manifested in politics through the Truth and Reconciliation Commission (TRC) in post apartheid era as a healing of the past injustice.[1746] *Ubuntu* has also manifested in business and other aspects of life. However its application in business has raised serious debates.[1747] More importantly *Ubuntu* has been somewhat inserted in the South African Constitution of 1996 and above all, it has already become part of constitutional jurisprudence of South African courts.[1748] There is now a handful of case law which has been decided in the spirit of *Ubuntu*.[1749]

The last point deserving mention is about HIV/Aids pandemic. South Africa is the most African country affected by HIV/Aids. By 2011 it was estimated that the overall HIV prevalence rate was approximately 10.6%.[1750] The total number of people lived with HIV was 5.38 million.[1751] An estimated 16.6% of the adult population aged 15-49 years was HIV positive.[1752] The number of new infections for 2011 among the population aged 15 years and older was estimated at 316, 900.[1753] An estimated 63,600 new HIV infections was among children aged 0-14 years.[1754] The South African government has been adopting various measures to curb the increasing number of

[1742] See e.g., Louw, J., 'Culture and Self in South Africa: Individualism-Collectivism Predictions', The Journal of Social Psychology, 2000, Vol.140, No.2, pp.210-217; Vogt, L and Laher, S., 'The Five Factor Model of Personality and Individualism/Collectivism in South Africa: An Exploratory Study', Psychology in Society, 2009, No.37, pp.39-54.
[1743] Hofstede Cultural Dimensions Summary,
http://www.clearlycultural.com/geert-hofstede-cultural-dimensions/individualism/ last visited 8/04/2012.
[1744] International Business Wiki,
http://internationalbusiness.wikia.com/wiki/South_Africa_Collectivism_vs._Individualism last visited 8/04/2012.
[1745] Ibid.
[1746] See e.g., Gade, C.B.N., '*Ubuntu* and the South African Truth and Reconciliation Process', M.A Thesis, Aarhus University, Denmark, 2010.
[1747] See e.g., MacDonald, D.A., '*Ubuntu* bashing: the marketisation of "African values" in South Africa', Review in South African Political Economy, 2010, Vol.37, No.124, pp.139-152.
[1748] See e.g., Keevy, I., '*Ubuntu* versus the Core Values of the South African Constitution', Journal for Juridical Science, 2009, Vol. 34, No.2, pp.19-58; Makgoro, J.Y., '*Ubuntu* and the Law in South Africa', Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, 1998, Vol. 1, No. 1, pp.1-11; Wing, pp.349-375, note 1155, supra.
[1749] Ibid.
[1750] Statistics of South Africa, Mid-Year Population Estimates, 2011.
[1751] Ibid.
[1752] Ibid.
[1753] Ibid.
[1754] Ibid.

new infections, providing health care for the victims of HIV/Aids pandemic, etc.[1755] However such measures have been considered by commentators as not sufficient.[1756]

Internationally, South Africa is a member of the United Nations (UN), African Union (AU) and SADC. Accordingly, international obligations from these organisations are applicable on South Africa.

6.3 Social Attitudes to Privacy

There are no general surveys as to privacy attitudes in South Africa. However public concern for privacy and data protection is positive and relatively high in South Africa. There is a large degree of consensus among experts in the field that one reason that has nourished privacy concerns in South Africa rests upon the legacy of apartheid regime.[1757] This position is partly justified by the founding provisions of the South African Constitution 1996. To be sure, Art (1) (a) sets out human dignity, the achievement of equality and the advancement of human rights and freedoms as one of the basic tenets of the Constitution. Moreover, Art (1) (b) categorically sets another pillar of the South African Constitution in the following words: 'no-racialism and no-sexism'. Examples of the scholarships that have given a clear linkage between claim for privacy and apartheid in South Africa are Wasserman and Boloka.[1758] These authors assert that while on the one hand there are laws indicating a general climate of openness and access to information in South Africa after 1994(i.e. after apartheid era), the issue of the media's invasion of politicians' privacy is raised in the Constitution itself.[1759] Hence the balance between privacy and freedom of information has been complicated by the past experiences of apartheid.[1760]

Besides the political arena, public concerns for individual privacy in South Africa have frequently been raised in the context of the operation of South African intelligence services. The apartheid state intelligence services of the early 1990s characteristically invaded the privacy of individuals; conducted various forms of surveillance without judicial authorisation; were unaccountable to

---

[1755] See e.g., Grundlingh, L., 'Government Responses to HIV/AIDS in South Africa as Reported in the Media, 1983-1994', South African Historical Journal, 2001, Vol.45, No.1, pp.124-154; New York Times., 'South Africa Redoubles Efforts Against AIDS', published 25th April 2010, http://www.nytimes.com/2010/04/26/health/policy/26safrica.html?pagewanted=all last visited 8/04/2012.

[1756] See e.g., Jordan, S., 'South Africa: How the government's response to HIV fails to address masculinity', http://www.kit.nl/net/KIT_Publicaties_output/ShowFile2.aspx?e=1040 last visited 8/04/2012.

[1757] See e.g., Banisar, note 1314, supra; Bygrave, p.343, note 25, supra.

[1758] Wasserman, H and Boloka, M., 'Privacy, the Press and the Public Interest in Post-Apartheid South Africa', Parliamentary Affairs, 2004, Vol.57, No.1, pp.185-195.

[1759] Ibid, p.189.

[1760] Ibid, pp.190-193.

parliament; and were involved in political violence, suppression and the manipulation of the domestic political environment.[1761] On this account, the historical antagonism and mistrust between the intelligence community and the population continues to have an impact on public perceptions of intelligence in South Africa in post apartheid era.[1762] Concerns for privacy as a result of fears of intelligence services can be demonstrated partly by the blog debates and comments on the thread '*I am a RICA criminal*'[1763] posted on 2 July 2009 by Arthur Goldstuck in the context of mandatory requirement for registration of SIM cards in South Africa. This became effective from 1 July 2009. Following an amendment of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 2002,[1764] South Africa requires service providers to register SIM cards of their subscribers. This legal requirement sparked a lot of discussion including '*I am a RICA criminal*'. The latter received a total number of 50 comments, many of them raising privacy concerns. It is imperative to quote some of these comments to illustrate how pertinent is the privacy issue in South Africa:-

> 'Richard
> This article, although at times somewhat inaccurate, does a magnificent job of illuminating the fine print of the Bill that was initially passed six years ago and has subsequently (and rather suspiciously) been kept in the dark. It really worries me that there seems to be such an apathetic and unengaged response from the general public when this Act, on face value, is blatantly threatening every mobile phone user's privacy of conversation and location. Sadly the "reasonableness-" criterion leaves a great deal up to the (easily corrupted) discretion of law enforcement (or am I being too cynical?) Should this fundamental right take a backseat because of the misdirection towards convenience? Jul 22nd, 2009.
>
> Joe Blogs
> The thing that gets to me is the fact that like most of the current legislation passed does not go out for public opinion or debate. this is just a clear example of how our government prefers to adopt the constitution when its suits them and to ignore it when they want to. Last that i looked, each and every South African had a right to privacy as stated as one of the key heading in the constitution. So really I don't care whether this was implemented by the Department of Justice or even the president, all

[1761] Hutton, L., 'Looking Beneath the Cloak: An Analysis of Intelligence Governance in South Africa', Institute for Security Studies (ISS), 2007, Paper No. 154, pp.1-24, at p.3.
[1762] Ibid.
[1763] Goldstuck, A., 'I am a RICA criminal', The Big Change, 2009, http://thebigchange.com/i-am-a-rica-criminal/ last visited 9/04/2012.
[1764] Act No. 70 of 2002.

of us as South Africans have a right to privacy and by implementing a law whereby any South African can be listened into at any given time and wit any prior notice is just not on. If I wanted to live in a country where the rights of people are not respected, then I would have moved to Zimbabwe. Mr. Zuma it may a good idea for both you and your cabinet to spend sometime there, maybe then you will learn what not to do as a president. Currently my concern is that we are heading in the direction of a Uncle Bob dictatorship. Aug 7th, 2009.

Aaron Scheiner
Great article! I'm trying to find ways of being able to give up my cellphone… one of them is using a UHF carrier to a VOIP line. I really do hope people make a stand against this.Oct 6th, 2009.

Ernie
This whole RICA thing is a direct invasion of our right to privacy and is against the constitution. Oh but I suppose that doesn't matter to this government as the constitution means nothing to them. I will not register my sim card period and if they cut my line I will take the matter to the constitutional court. I am tired of being abused by this government. While criminals walk free on our streets shooting innocent people for their cars, they waste money on crap like this is instead of focusing on the real issues we face in this country. It is about time we as South Africans stand together against this sort of abuse. Oct 8th, 2009.

Harold
the constitution states that every person has the right to privacy, that includes not to have their right to privacy of communication infringed. What I wonder is how was this law passed because when a is in conflict with the constitution it is automatically invalid. Nov 7th, 2009.

Craig
Heres an idea. Lets everyone just stop using cell phones and by implication stop paying the service providers. Then you will see how quickly the service providers get this nonsense sorted out with government. Hit them where it hurts, in the pocket.
Nov 12th, 2009.

Bob

Apart from victimising law abiding citizens once again, I think our clueless MPs will have successfully made a measurable contribution to our annual murder score. Think on it, owners of registered phones are potential targets for serious crime. If a criminal needs a cell number for a few days, then a simple mugging will only suffice for about 24 hours before the cel is reported stolen and the sim is locked. But on the other hand, if the victim is in no condition to report the loss of his/her rica registered phone…? Dec 28th, 2009.

Yasser

I am waiting for cellc to cancel my contract and then…..cause i am not going to register. For anything. hats this now…the white man was right when he told me, "any country that is govern by a black man is a mess" that is what's happening to this country. Rica what's next….vica?
Mar 5th, 2010.

Andries

This feels like another step has been taken in, as posted earlier, "keep civilians safe behind lock and key". I fear infringement of societies rights in order to prohibit criminal intent will only spark further criminal action by individuals/groups already living outside law-abiding society... Aug 23rd, 2010.

Crap

Well, what does one expect other useless law from the kaffirs. All they can do is come up with stupid ideas, showing the rest of the world how useless black government really is. They line the pockets every day, the country is going for a ball of shit. Rica my phone, never. it is so easy to get round it, and they are too stupid to realise it. Screw the kaffis.Oct 1st, 2010.

Stefan

Great article, thanks for the legal detail. I would love to see some opposition to this law mustered. I don't trust any government, let alone the ANC with it's glorious track record of corruption, with monitoring my phone calls – whatever the justification. Get lost RICA. I'll never register my sim card just to be under their thumbs. It seems obvious to me that this whole "deadline" and mass of scare tactics is to gauge how many people actually are subservient and how far the ANC can push civil rights and constitution down the toilet. I say don't register, you know they'll postpone the

> deadline anyway! No way the cell phone companies will cut the service of more than 100 000 people in one week! Their shares will plummet on that news and I will be there for the short. No doubt some hot-shot lawyer will build his career of fighting off this evil. Who's up to it? Oct 5th, 2010.
>
> Marius
> I agree, this law is there to control the public and not to catch criminals, this law might even increase cell phone theft since the value of a stolen or lost SIM card will make it a much better business than before. Thieves with thrive on stolen or abandon sim cards while the original owners will be held accountable. Jun 15th, 2011.'

The above concerns with regard to interception of private communication by intelligence services have not remained unreal. They have manifested in the recent high profile scandal charging the South African intelligence services of phone hacking without authorised orders of a judge.[1765] This has raised public fears over the spying laws.[1766]

Interception of private communication has not only been confined to the public sphere. Private firms as well as individuals have also been condemned of making unlawful interference of private communication. A handful of case law determined by the South African courts illustrate how public fears about their loss of privacy from private firms and individuals. Some of such cases include: *Financial Mail (Pty) Ltd v Sage Holdings Ltd;*[1767] *Bernstein v Bester NO;*[1768] *Protea Technology Limited and Another v Wainer and Others;*[1769] *S v Kidson;*[1770] and *Waste Products Utilisation (Pty) Ltd v Wilkes and Another.*[1771]

HIV/Aids has also raised a lot of concerns for privacy in South Africa. The manifestations of these concerns have resulted in a large corpus of case law by South African courts. The first of these cases concerned unauthorised disclosure of the patient's HIV status by the doctor in the famous *'McGeary case'* officially cited as *Jansen van Vuuren v Kruger.*[1772] In this case the court decided in favour of the patient. However, it is important to stress that HIV/Aids issues are

[1765] CAJ News Agency., 'SA Intelligence Faces Phone Hacking Scandal', http://cajnewsagency.com/index.php/technology/software/127-sa-intelligence-faces-phone-hacking-scandal, last visited 10/04/2012.
[1766] Ibid.
[1767] 1993 (2) SA 451(A).
[1768] 1996(2) SA (A); (2) SA 751 (CC).
[1769] [1997] 3 All SA 594.
[1770] 1999(1) SACR 338(W).
[1771] 2003(2) SA 515(W).
[1772] 1993(4) SA 342.

often racially determined in South Africa due to the apartheid experience.[1773] The *McGeary* case took place in 1993, and it involved a white, middle class man.[1774] However, it took 15 years later for the South African court to defend the right of the HIV/Aids status confidentiality of a black.[1775] This case famously known as the *De Lille case* (*NM and Others v Smith and Others*) involved three women who were HIV positive.[1776] Their status was detected in a clinical trial in which they participated. Subsequently, their full names with their related HIV status were published in the biography of Patricia De Lille which was authored by Charlene Smith and published by the New Africa Books. The publication was made without the three women's consent. Other cases on HIV/Aids in South Africa include: *Joy Mining Machinery v NUMSA and Others;*[1777] *I & J Ltd v Trawler & Line Fishing Union and Others;*[1778] and *PFG Building Glass (Pty) Ltd v Chemical Engineering Pulp Paper Wood and Allied Workers Union and Others.*[1779]

Commentators like Ndebele *et al*, have argued that HIV/Aids have reduced the relevance of the principle of individual medical confidentiality among the *Bantu* (i.e. Black) people of Southern Africa.[1780] These authors assert that due to *Ubuntu* which undermines the notion of individual autonomy, individual medical confidentiality does not work well with *Ubuntu,* which emphasises family, community, and sharing and solving of life problems together.[1781] Accordingly, there is frequent sharing and disclosures of HIV status of individuals to their family and community members. The view by Ndebele *et al*, is somewhat overstated. For example, the *De Lille case* illustrates the opposite, where disclosure of HIV status of blacks was strongly battled in court. Moreover such view does not fare well in the analyses of Olinger *et at.*[1782] Although the latter have found that there is little or no *Ubuntu* influence in the adoption of the data privacy legislation in South Africa suggesting similar position as Ndebele *et al*, they have not made any suggestion that once the data privacy law is adopted in South Africa it will apply to non-black population. As alluded to, the totality of the experience of apartheid has catalysed those who suffered under the regime, particularly the blacks, to be more privacy conscious and claim for their basic freedom and individual rights. Yet, caution has to be exercised not to generalise

[1773] Gorska, Z.M., 'Privacy, Surveillance and HIV/Aids in the Workplace: A South African Case Study', M.A Thesis, University of Witwatersrand, Johannesburg, 2008, p.36.
[1774] Ibid.
[1775] Ibid.
[1776] 2007(5) SA 250.
[1777] (2002) 4 BLL 372 (LC).
[1778] (2003) 24 ILJ 565(LC).
[1779] (2003) 24 ILJ 974(LC).
[1780] Ndebele, P *et al*., 'HIV/Aids reduces the relevance of the principle of individual medical confidentiality among the Bantu people of Southern Africa', Theoretical Medicine and Bioethics, 2008, Vol.29, No. 5, pp.331-340, p.331.
[1781] Ibid, p.337.
[1782] Olinger *et al*, note 64, supra.

situations. For example, when asked 'to what extent did the Department take into account cultural sensitivities when drafting the Bill' during the briefing meeting of the Justice and Constitutional Development and South African Law Reform Commission on the one hand and the Portfolio Committee on Justice and Constitutional Development on the other, Ms. Ananda Louw, Principal State Law Advisor for South African Law Reform Commission replied 'that each person had a conception of what privacy was. Some people would argue that one had no privacy. If a person signed up for Facebook, then one had no privacy. What the department found in all the different cultures was that if one had a lovely face, one did not mind having a picture of one's face taken, but if one had ugly legs then one would not want a person to take a picture of those legs. Something was private if the person concerned regarded it as being private. The law was there to protect those who indicated that they want their privacy protected.'[1783] Ms. Louw's reply clearly shows that values to privacy in South Africa significantly varies from one individual to another based on a vast array of factors such as the benefit such individual expect in return of his or her release of personal information.

There are similarly concerns for privacy arising from unsolicited marketing practices. During an interview with Sedibane Thabo in Pretoria, he had the following to say, 'since today we have to register our SIM cards, I propose or suggest that our personal information should be protected in order to prevent abuse. Marketing companies should not be allowed to access our personal information e.g. selling their products via cell phones.'[1784] This response supports the view by Ms. Louw that the Department faced many problems with the Direct Marketing Council during consultations because it largely deals with Spam mails.[1785] Perhaps one of the most appealing headlines that had raised the eyebrow of South Africans' concerns for privacy in the field of marketing practices was the announcement by the South African Post that it would sell the personal information of all registered citizens contained in its National Address Database (NAD).[1786] The NAD contained personal information about individuals' names, national identity numbers, home addresses, postal addresses as well as telephone numbers.[1787]

[1783]Parliamentary Monitoring Group (PMG)., 'Protection of Personal Information Bill [B9-2009] briefing', 6th October 2009,
http://www.pmg.org.za/report/20091006-protection-personal-information-bill-b9-2009-briefing,
last visited 11/04/2012.

[1784] Interview held on 29th June 2011, Pretoria, South Africa between the researcher of this thesis and Sedibane Thabo.

[1785] PMG, note 1783, supra.

[1786] Pretoria News, 15th June 2005 cited in Olinger *et al*, p. 32, note 64, supra.

[1787] Ibid.

However, it is interesting to note that CCTV cameras have generated limited privacy concerns in South Africa although the extensive use of CCTV technique is leading South Africa into a surveillance society.[1788] Currently in South Africa, CCTV is used in almost commercial venues such as hotels, casinos, banks, retail stores, airports, financial institutions, mines, garages, hospitals and shopping centres.[1789] Yet, despite this extensive use of CCTV cameras there have been no strong opposition of their use by the public as it has been the case in Europe.[1790] Very probably, this is because of the crime rate, which is enormous in South Africa compared to that of Germany (and Europe generally); because of the perceived immediate threat it presents; and because of the population in general is more prepared to submit to the relatively far-ranging curtailments of the protection of their private sphere.[1791] This view is tandem to the response the researcher of this thesis received from Professor Roos that while South Africans are concerned about invasion of their privacy when information is required from them, they are at the same time ready to give out their personal information if they feel they will get a benefit in return.[1792]

6.4 Legal and Regulatory Framework

At present, privacy in South Africa is protected through the Constitution 1996, common law and legislative frameworks. The first two sources of law are of general nature and in which case more prevalent while the third source is more context specific. As alluded to, these sources are not considered as adequate to protect personal information in a similar manner as data protection legislation. Partly because of this deficiency, South Africa has decided to adopt a comprehensive data protection law which is still being considered by the Portfolio Committee on Justice and Constitutional Development of the South African Parliament. This part provides a lengthy discussion and analysis of this Bill. The other sources are only analysed to show how strong and weak they are in specific contexts. It is also important to mention that the constitutional and common law source of privacy protection in South Africa have been extensively dealt by renowned South African scholars such as Professor Anneliese Roos, Professor Johann Neethling

[1788] The term 'surveillance' is in this context assigned a wider meaning to include both the activities of the public and private sector with regard to processing of an individual's personal data.
[1789] Van Rensburg. J., 'CCTV Security and Safety Security/Safety Equipment – Africa', International Market Insight. 2001, Strategis: Industry Canada, cited in Norris, C *et al.*, 'Editorial: The Growth of CCTV: A Global Perspective on the International Diffusion of Video Surveillance in Public Accessible Space' Surveillance and Society, 2004, 2(2/3), pp.110-135, at p.115.
[1790] Hörner, S., 'Datenschutz und Kriminalitätsprävention in Südafrika Ein Vergleich mit Deutschland am Beispiel der Einführung der Videoüberwachung öffentlicher Plätze', KAS-AI 11/04, S.62-88, at p. 63, http://www.kas.de/wf/doc/kas_5813-544-1-30.pdf?041213120312 last visited 11/04/2012.
[1791] Ibid, p.66.
[1792] Interview held between the researcher of this thesis and Professor Anneliese Roos on 28th June 2011, Pretoria, South Africa.

et al and Professor Max Loubser *et al*. Since most of these works present the correct account of the law, this thesis limits lengthy discussion on the same issue.

6.4. 1 The Constitution of South Africa 1996

The Constitution of South Africa 1996[1793] was promulgated on 18 December 1996 and officially commenced to apply as from 4 February 1997. One of the significant changes brought by the South African Constitution 1996 was the repeal of the Constitution of the Republic of South Africa 1993.[1794] The latter was an interim Constitution towards the majority rule in South Africa which marked the end of apartheid era. The Interim Constitution was assented on 25 January 1994 and commenced to apply on 27 April 1994. Because of this, it is sometimes loosely referred as Constitution of South Africa 1994.

Privacy is constitutionally protected in South Africa. It has been protected as a fundamental right in South African Constitutions since 1994.[1795] Section 13 of the Interim Constitution provided, 'every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violation of private communications.' This provision has been reproduced with insignificant modifications in the South African Constitution 1996. It appears in section 14 as follows:-

> 'Everyone has the right to privacy, which includes the right not to have-
> (a) their person or home searched;
> (b) their property searched;
> (c) their possession seized;
> (d) the privacy of their communications infringed.'

The above section is apparently narrow in scope of protection in the sense that it guarantees a general right to privacy, with specific protection against searches and seizures and of the privacy of communications.[1796] However it has been argued that the list of privacy instances provided in section 14 of the South African Constitution 1996 is not exhaustive: the protection given by this right extends to any other method of obtaining information or making unauthorised

[1793] Act No. 108 of 1996.
[1794] Act No. 200 of 1993; see the Seventh Schedule.
[1795] Roos, p.352, note 201, supra.
[1796] Ibid, p.353.

disclosures.[1797] Accordingly, while the instances of privacy enumerated in section 14 of the Constitution 1996 relate to the 'informational' aspects of the right to privacy, courts have extended the right to privacy to 'substantive' privacy rights.[1798] The latter are rights which enable persons to make decisions about their family, home and sexual life.[1799]

At the same time, the right to privacy in the South African Constitution is broad in two respects. First, the fact that section 14 opens with the expression 'everyone' suggests that the protection afforded in this section extends to non-South African citizens. This is similar to the European Directive 95/46/EC which is not restrictive of protecting privacy of EU citizens only. The other aspect regarding the broad scope of constitutional privacy under the South African law is that it applies to both natural/physical as well as juristic persons. Section 8(2) of the Constitution states that 'a provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by their right.' This means that data controllers who are most invariably corporations are subject of the provision of section 14 of the Constitution as to the enjoyment of the privacy right. However, this right is only limited. Section 8(4) of the Constitution provides the limitation of privacy right afforded to juristic persons as follows, 'a juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person.' In the case of *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty); In re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO*, the Constitutional Court of South Africa held:-

> 'Juristic persons are not the bearers of human dignity. Their privacy rights, therefore, can never be as intense as those of human beings. However, this does not mean that juristic persons are not protected by the right to privacy. Exclusion of juristic persons would lead to the possibility of grave violations of privacy in our society, with serious implications for the conduct of affairs....'[1800]

[1797] McQuoid-Mason, D.J., 'Privacy' in Chaskalson, M *et al*,(eds)., Constitutional Law of South Africa, Juta, Kenwyn, 1996, 18-11, cited in Roos, p.353, note 201, supra.
[1798] Roos, p.353, note 201, supra.
[1799] Ibid; see also Neethling *et al*., (Neethling's Law of Personality), p.220, note 186, supra; De Reuck v Director of Public Prosecutions, Witwatersrand Local Division 2004(1) SA 406(CC); Bernstein v Bester NO 1996 (2) SA 751 (CC).
[1800] 2001 1 SA 545 (CC) 557. For detailed discussion of the right to privacy for juristic persons in South Africa see, e.g., Roos(LL.D Thesis), pp.639-643, note 2, supra; Neethling *et al*, (Neethling's Law of Personality), pp.68-73, note 186, supra.

It is imperative to note that the constitutional right to privacy is not absolute. In order to balance it with the exercise of other rights and interests, it is limited by section 36(1) of the Constitution. Under this section, the rights in the Bill of Rights including the right to privacy, may be limited only in terms of the general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors. The latter include the nature of the right; the importance of the purpose of the limitation; the nature and extent of the limitation; the relation between the limitation and its purpose; and less restrictive means to achieve the purpose. Beyond the limits provided in section 36(1) or any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights in the South African Constitution 1996.[1801] This means that the question of infringement of the constitutional right to privacy must be investigated by a two-stage approach. First, whether an individual's right to privacy has been interfered and second, whether such interference is justified under the limitation in section 36(1) or any other provision of the Constitution.

As pointed out, section 39 of the South African constitution provides guidance on how courts, tribunals or forums should interpret the provisions of the Bill of Rights. In their interpretation, courts, tribunals or forums must promote the values basic to an open and democratic community based on human dignity, equality and freedom. They must also take into account international law and may consider foreign law.[1802] The latter include both decisions of foreign national courts or foreign national legislation.[1803] Also, when interpreting any legislation, and developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights. Moreover, the Bill of Rights does not deny the existence of any other rights or freedoms that are recognised or conferred by common law, customary law or legislation, to the extent that they are consistent with the Bill. What it means is that the Bill of Rights sets the standard upon which the existence of other rights from other sources of laws is measured up.

It can be submitted that although it is generally argued that the protection of privacy afforded by the Constitution is not the same as the data protection legislation,[1804] the recognition of privacy as a fundamental right in the South African Constitution 1996 serves two significant purposes. It

[1801] The Constitution of South Africa 1996, s. 36(2).
[1802] The Constitution of South Africa 1996, s. 233.
[1803] Church*, et al.*, p.194, note 159, supra.
[1804] Gorska, p.31, note 1773, supra.

prevents the legislature and the executive of the state from passing any law or taking any action which infringes or unreasonably limits the right to privacy.[1805] Also, the entrenchment of privacy in the Constitution gives it a higher status in that all law, state actions, court decisions and even the conduct of natural and juristic person may be tested against.[1806]

6.4.2 The Common Law

The common law provides the earliest source of privacy protection in South Africa. There is a considerable degree of consensus among South African commentators that the current protection of privacy in the South African Constitution 1996 is merely the codification of the common law protection of privacy although some differences can still be made.[1807] At common law, privacy is recognised as a personality interest and protected by the law of *delict*.[1808] Similar to the English law, the functions of *delict* 'are those purposes or ends which people seek to further or achieve through tort law'.[1809] Compensation for harm is the primary, but not the sole function of the law of *delict*.[1810] Yet, unlike the English law which is focused on specific torts, the South African law on delictual liability is based on general principles.[1811] Due to this, the latter is more flexible than the former in the sense that it is able to accommodate changing circumstances and new situations without necessarily creating new delicts which is a slow legislative process.[1812] The South African law of *delict*, unlike the English law of torts, has therefore been able to recognise and protect individual interests such as privacy and the goodwill of a corporation which have only come to the force in modern times.[1813]

The classical case for the recognition of an independent right to privacy in South African law is *O'Keeffe v Argus Printing and Publishing Co Ltd.*[1814] The brief facts in *O'Keeffe* were that, a woman had agreed to be photographed and her likeness to be used as part of a news article. In contrast, her photograph was used in an advertisement for rifles, pistols and ammunition. In finding for the claimant, the court took a broad view that *dignitas* (i.e. dignity) does not represent a single interest

---

[1805] Neethling *et al*, (Neethling's Law of Personality), p.17, note 186, supra.
[1806] Ibid, p.75.
[1807] See e.g., Roos, p.355, note 201, supra; Neethling *et al*, (Neethling's Law of Personality), p.220, note 186, supra.
[1808] Ibid(Roos); see also Roos,(LL.D Thesis), chapter 7, note 2, supra; Neethling *et al*, (Neethling's Law of Personality), chapter 8, note 186, supra; Neethling *et al*., (Law of Delict), note 186, supra; Loubser, M *et al*., The Law of *Delict* in South Africa, Oxford University Press Southern Africa, Cape Town, 2010.
[1809] Loubser *et al*., p.8, note 1808, supra.
[1810] Ibid.
[1811] Neethling *et al*., (Law of *Delict*), p.4, note 186, supra
[1812] Van der Walt, J.C and Midgley, J.R., Principles of *Delict*, Butterworths, South Africa, 2005, p.31 cited in Neethling *et al*., (Law of *Delict*), p.5, note 186, supra.
[1813] Neethling *et al*., (Law of *Delict*), note 1812, supra.
[1814] 1954 (3) SA 244(C).

of personality (namely dignity which is infringed by insult), but as the whole legally protected personality-or all 'those rights relating to...dignity-except *corpus* (i.e. bodily integrity) and *fama* (i.e. reputation).[1815] Accordingly the court correctly found privacy as one of such rights falling under *dignitas*.[1816] In *Jansen van Vuuren v Kruger,*[1817] the Appellate Division held that 'the *actio iniuriarum* (i.e. a legal action for violation of a personal interest) protects a person's *dignitas* and *dignitas* embraces privacy.

As alluded to, in South Africa privacy is also protected under the common law of *delict*. A *delict* is the act of a person that in a wrongful and culpable way causes harm to another.[1818] While privacy is generally said to be infringed when someone learns of true private facts about another person against his or her determination and will,[1819] in order to succeed in a claim for privacy infringement a claimant has to prove the five elements in the definition of a *delict*: act or conduct, wrongfulness, fault, causation and harm.[1820]

By act or conduct it means a voluntary human act or omission.[1821] This means that only an act of a human being in contrast to that of an animal is accepted as 'conduct'.[1822] Where a human being uses an animal as an instrument in the commission of a delict, a human act is still present.[1823] Moreover it is acceptable that a juristic person may act through its organs (humans) and may thus be held delictually liable for such actions.[1824] Once an act or omission is established, the claimant has to prove that it was wrongful. By wrongful it simply means that an act or conduct has its consequence the factual infringement of his or her personal interest, in this case privacy.[1825] Fault is the legal blameworthiness or the reprehensible state of mind or conduct of someone who acted wrongfully.[1826] Its main forms are intention and negligence.[1827] However for purposes of the *actio iniuriarum* intention is generally required and negligence is insufficient to sustain liability.[1828] Apart from proving that an act or conduct was wrongful and the defendant was at fault, it has to be further proved that the damage or harm resulted from the conduct of

[1815] Neethling *et al.*, (Neethling's Law of Personality), p.217, note 186, supra.
[1816] Ibid.
[1817] 1993(4) SA 842(A), p.849.
[1818] Neethling *et al.*, note 1811, supra.
[1819] Ibid, p.347.
[1820] Ibid, note 1811.
[1821] Ibid, chapter 2.
[1822] Ibid, p.25.
[1823] Ibid.
[1824] Ibid.
[1825] Ibid, p.34 (and generally chapter 3).
[1826] Ibid, p.123 (and generally chapter 4).
[1827] Ibid.
[1828] Ibid, p.124.

the defendant.[1829] In other words, a causal nexus between conduct and damage is required for a *delict*.[1830] Finally, the claimant has to prove harm.[1831] As pointed out, the primary function of the law of *delict* is compensatory. Hence to establish a delictual liability the claimant has to prove that he or she had suffered some loss or damage from another person's wrongful act or conduct.[1832]

However, there are set of grounds of justification which may negative the wrongfulness element of an act or conduct. These operate as general defences. They include such grounds as consent, necessity, provocation, statutory authority, official capacity, obedience to orders, disciplinary powers and impossibility.[1833] Yet, not all these grounds of justification are applicable in the context of privacy infringement and consequently relevant for data protection.[1834] Consent is especially relevant when infringement of privacy is involved.[1835] This is so because the individual determines what he or she considers to be private and 'absent a will to keep a fact private, absent an interest (or right) that can be protected.[1836] Other defences relevant to privacy infringement include necessity, statutory authority, official capacity and public interest.[1837] There is also the defence of impossibility.[1838] The rest of the general defences of common law of *delict* are not applicable in claims for privacy infringement.

As is the case with the constitutional protection, the common law protection of privacy through *delict* is broad. It applies to everyone irrespective of its citizenship.[1839] However it generally falls short of the general principles of data protection.[1840]

6.4.3 The Data Protection Bill 2009

The Protection of Personal Information Bill 2009 (simply abbreviated PPIA after the name of the Act to be enacted or Data Protection Bill) constitutes South Africa's latest efforts to adopt comprehensive data privacy legislation.[1841] The Bill was introduced for the first reading in the Parliament of South Africa on 25 August 2009. Subsequently on 6 October 2009, it was sent to

[1829] Ibid, chapter 5.
[1830] Ibid, p.175.
[1831] Ibid, chapter 6.
[1832] Ibid, p.211.
[1833] Loubser *et al.*, chapter 9, note 1808.
[1834] Roos,(LL.D Thesis), p.590, note 2, supra
[1835] Ibid, 591.
[1836] Ibid.
[1837] Ibid, pp.595-599.
[1838] Ibid, p.599.
[1839] Ibid, p.547.
[1840] See e.g., Roos, note 201, supra.
[1841] Bill No. 9 of 2009.

the Portfolio Committee on Justice and Constitutional Development for deliberations and considerations before it is adopted as law by the Parliament. Until 29 March 2012 there were six working drafts of the Data Protection Bill. The seventh and the final version is currently being prepared by the Technical Sub-Committee for the Portfolio Committee on Justice and Constitutional Development. The subsequent analyses will therefore rely much on the Sixth Working Draft of the Bill.[1842] This is because, the final version of the Bill as deliberated by the Portfolio Committee will be the one to be debated by the Parliament in its second reading. However some comparison with the original Bill will be made where necessary to show to what extent the original Bill has transformed.

Essentially, the Data Protection Bill proposes a law on regulation of processing of personal data similar to EU Directive 95/46/EC. The Bill contains the basic principles of data processing as well as a centralised authority for its implementation. It proposes to amend certain existing legislation which currently applies in specific data processing contexts. The latter are considered in 6.4.5.

6.4.3.1 Need for Data Protection Legislation

There are three main sources of accounts as to why South Africa decided to propose a Bill on data protection. The first of these sources is the memorandum on the objects of the Bill itself. The second source is *travaux préparatoires*. The latter source manifests in the records of the South African Law Reform Commission (SALRC) and deliberations of the Portfolio Committee on Justice and Constitutional Development. The third source comprises of scholarly works of South African commentators. While sometimes the reasons offered in these strands are similar, they are at times different not only in their scope but also in their contents. Due to this, it is appropriate to deal with them together while pointing out the main areas of their divergences.

The Memorandum on the Objects of the Protection of Personal Information Bill 2009 states two purposes for the Bill. First, it provides that the Bill aims to give effect to the right to privacy, by introducing measures to ensure that the personal information of an individual (data subject) is safeguarded when it is processed by responsible parties.[1843] Second, the Bill aims to balance the right to privacy against other rights, particularly the right of access to information, and to

[1842] Dated 27th January 2012.
[1843] The Memorandum on the Objects of the Protection of Personal Information Bill 2009(appended to the Bill), paragraph 1.

generally protect important interests, including the free flow of information within and across the borders of South Africa.[1844]

The above twin objectives are reflected in the long title of the Data Protection Bill.[1845] They are further consolidated in the preamble to the Bill. The latter makes clear that the Bill is first and foremost premised on section 14 of the South African Constitution 1996 on protection of the right to privacy. This implies that the Data Protection Bill is an implementation of the privacy provision of the constitution. Second, the preamble categorically states that the Bill is adopted bearing in mind the need for economic and social progress within the framework of the information society which usually requires the removal of unnecessary impediments against the free flow of information including personal data. Third, the Bill is adopted in order to regulate the processing of personal information in harmony with international standards.

Perhaps to give more prominence, section 2 of the Data Protection Bill incorporates the spirit of the preamble of the Bill. This section is titled 'Purpose of the Act'.[1846] Moreover to ensure that the purposes stated in section 2 of the Bill are promoted and given considerable weight in the implementation of the Act once passed by Parliament, section 3(3) of the Data Protection Bill requires interpretation of the Act must always give effect to the purpose of the Act set out in section 2, and at the same time it does not prevent any public or private body from exercising or performing its powers, duties and functions as long as they are related to the purpose of the Act or any other legislation which regulates processing of personal information.

In the light of the above it can be submitted that, generally the agenda behind the proposition of the Data Protection Bill is twofold. First, it seeks to protect privacy. Second, the Bill seeks to secure economic gains for South Africa. Yet at this stage it is difficult to assess the relative

---

[1844] Ibid.

[1845] Bill to promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for processing of personal information; to provide for the establishments of an Information Regulator; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.

[1846] The purpose of this Act is to- (a)give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at-(i) balancing the right to privacy against other rights, particularly the right of access to information; and (ii) protecting important interests, including the free flow of information within the Republic and across international borders; (b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information; (c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and (d) establish voluntary and compulsory measures, including an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

strength of these agendas as to their influence in the proposed data privacy legislation. It is imperative to assess other sources of reasons behind the Data Protection Bill.

Perhaps the most comprehensive strand explaining the reasons why South Africa has proposed comprehensive data privacy legislation is comprised in the background paper for deliberations of the Portfolio Committee.[1847] This paper lists four main reasons why South Africa needs to adopt data privacy legislation. The first is the response to Parliamentary request.[1848] This request came as a result of the limitations for incorporating data privacy law in the then Open Democracy Bill. Accordingly the Parliamentary Ad Hoc Joint Committee on the Open Democracy Bill requested the Minister of Justice and Constitutional Development to introduce privacy and data protection legislation in Parliament, after thorough research of the matter, as soon as reasonably possible.[1849] The Committee pointed out that the Open Democracy Bill (as it then was, the Bill was later renamed and became the Promotion of Access to Information Act) dealt with access to personal information in the public and private sector to the extent that it included provisions regarding mandatory protection of the privacy of third parties.[1850] Similarly the Committee argued that the Bill did not, however, regulate other aspects of the right to privacy, such as the correction of and control over personal information and so forth.[1851] The Committee furthermore reported that foreign jurisdictions with access to information legislation have also enacted separate privacy and data protection legislation.[1852] Since the work of the Committee was subject to a constitutional deadline, the sections in the Bill dealing with privacy and protected disclosures were removed for consideration at a later stage.[1853]

The second reason advanced in the background paper proposing for the data privacy legislation is the constitutional imperative.[1854] This is the same reason as the one stated in the Memorandum of Objects of the Bill. The same is repeated in the long title of the Bill, preamble and section 2 of the proposed Bill. It is clear that in South Africa privacy is protected in terms of common law and section 14 of the Constitution. However the South African Constitution is the supreme law. Any law which is in conflict with the Constitution becomes invalid. In this way the common law is itself required to be in agreement with the provisions of the Constitution. Yet, constitutional

[1847] Portfolio Committee on Justice and Constitutional Development., 'Background Information: Protection of Personal Information Bill [B9-2009], Deliberations 4th November 2009; http://www.pmg.org.za/report/20091104-protection-personal-information-bill-b9-2009-deliberations last visited 15/04/2012.
[1848] Ibid, paragraph 2.1.
[1849] Ibid.
[1850] Ibid.
[1851] Ibid.
[1852] Ibid.
[1853] Ibid.
[1854] Ibid, paragraph 2.2.

protection of privacy is too broad. It does not embody data protection principles which regulate processing of personal data. Thus, the need to enact general data privacy legislation is to give effect to the constitutional protection of the right to privacy by creating specific privacy rules for data processing.

The third reason for adopting data protection legislation is to fulfil international obligations and expectations of trading partners.[1855] The Bill, as far as South Africa's international obligations are concerned, aims to create a statutory framework in terms of which the Republic will be able to comply with the expectations of its major trading partners relating to the processing of personal information.[1856] Therefore the Bill is in compliance with the following two crucial instruments: Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention); and the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[1857]

Moreover, the Bill seeks to meet EU adequacy requirements in terms of the Data Protection Directive 95/46/EC.[1858] The Directive provides that personal data should only be allowed to flow outside the boundaries of the European Union to countries that can guarantee an 'adequate level of protection' of the data.[1859] From a business perspective, an adequate privacy protection rating will result in the free flow of information, both nationally and internationally, which will stimulate the economy and provide employment opportunities, for instance in the call-centre industry.[1860] It also has major implications for credit granting and financial institutions, for hotel and airline reservations systems, for the direct marketing sector, for life and property insurance, for the pharmaceutical industry and for any online company that markets its products and services worldwide.[1861] Proper protection of privacy will also ensure consumer confidence and trust in electronic on-line business activities.[1862]

Similarly, the 'adequacy' and economic imperative reasons appear prominently in scholarly works of various commentators. Plückhahn, for example, posits:-

---

[1855] Ibid, paragraph 2.3.
[1856] Ibid.
[1857] Ibid.
[1858] Ibid.
[1859] Ibid.
[1860] Ibid.
[1861] Ibid.
[1862] Ibid.

> 'The need for a legislative data protection framework in South Africa is largely a trade and development issue. After the European Union introduced the Data Protection Directive (Directive 95/46/EC), it was deemed necessary by the South African government to place the issue of data protection on the agenda. This is due to the fact that the E.U Data Protection Directive sets out a standard that requires that all personal information of E.U citizens must be protected. This is a standard that all countries, that process data belonging to the E.U member states and its citizens, must adhere to.'[1863]

In respect to South Africa, one major issue that was taken into consideration was that any sort of legislation adopted to protect privacy in compliance to the European Directive should at the same time promote the country's economy.[1864] This view is supported by Ms. Louw who briefed the Portfolio Committee that the protection of information was not a domestic policy but a worldwide concern.[1865] She also briefed that the Bill was a hybrid piece of legislation incorporating the human right perspective while providing for economic expediencies.[1866] However, when she was asked what influenced African countries which have adopted the data privacy legislation, she pointed out, Europe.[1867] It was because of this that Ms. Louw contended that the data privacy legislation has primarily to be interpreted with reference to the international instruments from which it originated.[1868]

Similarly, in her 2004's article, Caroline Ncube argued as Plückhahn.[1869] At the same time, Roos has in different occasions considered economic imperative and compliance to the European Directive 95/46/EC as the agenda behind data privacy in South Africa. She argues that considering the international trend and expectations, information privacy or data legislation will ensure South Africa's future participation in the information market, if it is regarded as providing 'adequate' data protection by international standards.[1870] Roos has reiterated this view in a wider scope where she argues:-

---

[1863] Plückhahn, P., '(E-Commerce) Data Protection in the European Union and South Africa: A Comparative Study', Msc Thesis, Aarhus University (Denmark), 2010, p.62.
[1864] Ibid, p.64.
[1865] PMG, note 1783, supra.
[1866] Ibid.
[1867] Ibid.
[1868] Ibid.
[1869] Ncube, note 172, supra.
[1870] Roos, A., 'Data Protection Provisions in the Open Democracy Bill, 1997', Journal of Contemporary Roman-Dutch Law/Tydskrif Vir Hedendaagse Romein- Hollandse Reg (*THRHR*), 1998, Vol.61, No.3, pp.497-506, at p.499.

> 'The Directive...has an impact on South African businesses. The EU countries, who are subject to the Directive, are major partners of South Africa. Any impediment in the flow of information from Europe to South Africa will impact negatively on South Africa's participation in the global economy. As such, South Africa has to ensure that the protection afforded to personal information in South Africa is of an acceptable standard for the international community.'[1871]

The above scholarly views appear in the South African Law Reform Commission preparatory works on the Data Protection Bill. There is a considerable degree of consensus that economic imperative particularly trade is one of the agenda behind the adoption of data privacy legislation in South Africa. This may be expressly and impliedly discovered where the SALRC makes review of Articles 25 and 26 of the European Directive 95/46/EC with respect to the requirements of the 'adequacy' standards. The SALRC points that 'with the exception of the USA, the requirements set out in the EU Directive have resulted in growing pressure outside Europe for the passage of strong information protection laws. Those countries that refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive information.'[1872] Undoubtedly, South Africa is not an exception to this requirement as demonstrated by the SALRC, 'it is important to consider that the transfer of information to South Africa from Europe is governed from the European side by the Directive or country legislation that is implemented in terms of the Directive'.[1873] The issue is obviously of concern to business in South Africa.[1874] It is imperative to note that respondents to Issue Paper 24 were general in favour of the principle that care should be taken to ensure that South Africa satisfies the 'adequate standard' in terms of Art 25 of the European Directive 95/46/EC.[1875] Yet, there were differing views on the approach to meet the standard. Those who favoured a comprehensive data privacy statute particularly the Internet Service Providers Association argued as follows:-

> 'South Africa's international trade aspirations would be adversely affected by the adoption of a privacy model that is considered inadequate by international and EU standard. This impact would not be felt on a bilateral basis, but on the

[1871] Roos, pp.406-407, note 2, supra.
[1872] South African Law Reform Commission, Discussion Paper 109, paragraph 7.16, note 249, supra.
[1873] Ibid, paragraph 7.17.
[1874] Ibid.
[1875]Ibid, paragraph 7.18.

> multilateral level. It would result in lost opportunities for database warehousing, and possible crossborder trade in financial and telecommunications services. Moreover, as the SADC region moves towards a trade bloc in 2008, South Africa's policies should be a guiding best practice for the region and capable of adaptation by our regional trading partner.'[1876]

The Banking Council, Gerhard Loedolff, Nedbank, and Eskom Legal Department were some of the respondents who argued, 'it will definitely affect South African international trade negatively if we do not meet the requirements of article 25 of the EU Directive.'[1877] Nedbank has gone far to explain the extra costs she incurs due to lack of comprehensive data privacy legislation in South Africa. The bank has been forced with the absence of legislation to set up processing centres in Europe, in order to meet the European information protection legislative requirements.[1878] The bank faces similar difficulties that it is precluded from transferring personal information relating to its customers from its branches in London, Hong Kong, New York and other jurisdictions to its head office in South Africa, for the reason that South Africa has not yet adopted adequate information protection legislation.[1879]

Respondents who argued against the general data privacy law in the European style such as Sagie Nadasen Legal Adviser and Sanlam Life Law Service have argued that in case of satisfying the adequacy provision; South Africa can adopt self regulations and rely on courts' intervention.[1880] These respondents have similarly argued that 'both contractual provisions concluded between South Africa and foreign companies (which provisions will ensure that core principles and procedures are adequately addressed) and the existing Constitutional protection of fundamental freedoms and rights are more than sufficient to meet information protection concerns of the regulatory authorities in Europe. South African companies must of course ensure that any audit will confirm that they have requisite systems of and processes in place to meet the EU requirement of "adequate level of protection".'[1881] The strongest criticism against adoption of comprehensive privacy legislation aired by respondents can be summarised in the following paragraph:-

---

[1876] Ibid, paragraph 1.19.
[1877] Ibid.
[1878]Ibid.
[1879] Ibid.
[1880] Ibid, paragraph 7.20.
[1881] Ibid.

> 'The majority of African States, if not all, have no information privacy legislation in place and subjectively it is foreseen that with the problems of the continent being what they are, the introduction of such legislation will not be seen for some considerable time. South Africa is presently increasing its presence on the continent and many South African organisations have offices throughout Africa. In effect this will mean that South Africa would isolate itself from the rest of the continent in its attempt to blindly follow directives designed for economies far removed from Africa and South Africa.'[1882]

The fourth reason behind the adoption of the data protection legislation in South Africa is to address the mischief in the existing system of privacy protection.[1883] It is argued that the widely use of modern technologies has led to a considerable information explosion and has increased opportunities for private data collection.[1884] Some of the information collected may unduly harm the subject of the collection by undermining his or her dignity, integrity and independence as it may be inaccurate, incomplete, irrelevant, accessed and distributed unlawfully, used for purposes that are incompatible with and or contrary to the purpose for which it was collected or unlawfully destroyed.[1885] The challenges of modern technologies could not be addressed in by the common law of *delict* as well as section 14 of the Constitution 1996.

The preceding discussion reveals that protection of privacy and promotion of trade and business are the main agenda behind the proposition of data privacy legislation in South Africa. Although the Memorandum of Objects of the Bill, the long title, preamble and section 2 of the Bill make reference to economic progress as one of the agenda behind the data privacy law in South Africa, in relative terms, protection of privacy appears to be more a prominent agenda than securing trade and business. This can be noticed in the *travaux préparatoires* generally particularly those of the South African Law Reform Commission. Likewise, although commentators have pointed out the economic imperative as one of the reasons behind data privacy legislation in South Africa, most of their discussions are based upon privacy protection as such. Perhaps this is because of the country's long history of apartheid and the injustice that was brought about through the use of personal information. It is also significant to note that privacy has long been protected in South Africa through the common law of *delict*. As alluded to, *O'Keeffe* set the baseline for

---

[1882] Ibid.
[1883] Portfolio Committee on Justice and Constitutional Development, paragraph 2.4, note 1847, supra.
[1884] Ibid.
[1885] Ibid.

protection of privacy as an independent personality interest as far back as 1954. Subsequent to *O'Keeffe,* several cases based on infringement of the right to privacy have been considered and decided by the South African courts. Moreover, the incorporation of a specific provision for protection of privacy in the South African Interim Constitution 1994 and subsequently in the permanent South African Constitution 1996 strengthened privacy protection in the country. This is because, privacy has become a fundamental right. It can therefore be noted that even prior to the adoption of the European Directive 95/46/EC and its coming into force in 1998, South Africa had a fairly stronger system of privacy protection. Although the latter has not been adequate to protect processing of personal data in the present era of information technologies it has laid the foundation of adoption of the data privacy legislation. However despite that the influence of the European Directive 95/46/EC remains imminent as shown in the subsequent analyses.[1886]

6.4.3.2 Legislative Process

Data protection has been on South African legislative agenda since mid-1990s.[1887] Initially the provisions for regulating personal information appeared within the Open Democracy Bill 1996 which later became known as Promotion of Access to Information Act 2002(PAIA). Yet, these provisions did not fit well within the context of the Open Democracy Bill which was intended to promote governmental transparency through the access of information. Moreover the Bill was part of the efforts of the post-apartheid government to cure the secrecy with which the apartheid regime operated in South Africa rather than to regulate data processing. Partly due to this, it was viewed that the provisions regulating data protection be removed out of the Open Democracy Bill and reserved for a separate legislation. The Minister of Justice was requested by the Ad Hoc Joint Committee on the Open Democracy Bill to consider the introduction of such legislation in Parliament.[1888] This request was later referred by the Minister to the South African Law Reform Commission marking the beginning of the Commission's subsequent investigation into privacy and data protection legislation.[1889]

[1886] See also e.g., Allan, K and Currie, I., 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa', South Africa Journal on Human Rights, 2007, Vol. 23, No.3, pp. 563-579, at pp.563-572.
[1887] See e.g., Currie, p.2, note 248, supra; Allan and Currie, p.565, note 1869, supra.
[1888] Report of the Ad Hoc Joint Committee on the Open Democracy Bill [B67-98], 24th January 2000, http://www.parliament.gov.za/live/content.php?Item_ID=280#22 last visited 17/04/2012.
[1889] South African Law Reform Commission, Issue Paper 24, paragraph 1.1.4, note 250, supra.

At the request of the South African Law Reform Commission, the Minister appointed a Project Committee to assist the Commission in its task.[1890] The chairperson of the Committee was Honourable Mr. Justice Craig Howie. Prof. Johann Neethling was appointed as the project leader while other members included Prof. Iain Currie, Ms. Caroline da Silva, Ms. Christiane Duval, Prof. Brenda Grant, Ms. Adri Gobler, Mr. Mark Heyink, Ms. Saras Jogwanth and Ms.Allison Tilley.[1891] The Committee met for the first time on 22 July 2002.[1892]

The SALRC made extensive public consultations in its investigation.[1893] First, the Commission published the Issue Paper 24 in September 2009 with a set deadline on 1 December 2003.[1894] This was subsequently followed by the publication of the Discussion Paper 109 in October 2005 with a deadline on 28 February 2006 which was extended to 30 September 2006 at the public request.[1895] In addition, the Commission carried out regional workshops countrywide to discuss and explain to the public various options proposed for protection of their personal information.[1896] Based on the responses received from public on account of the Issue and Discussion Papers, the Commission prepared a comprehensive report with a proposed Bill on data privacy law.[1897] This report was submitted to the Minister of Justice and Constitutional Development and was made public on 26 August 2009.

As pointed out, the Protection of Personal Information Bill 2009 was introduced to the Parliament for its first reading on 25 August 2009. Subsequently, it was sent to the Portfolio Committee on Justice and Constitutional Development for deliberation and consideration. The

---

1890 Ibid, paragraph 1.1.5.
1891 Ibid.
1892 Ibid.
1893 However there were still some complaints particularly from Business Unit South Africa (BUSA) made to the Portfolio Committee on 13th October 2009 during public hearing that the consultation period by the SALRC was not sufficient, BUSA., 'Submission Protection of Personal Information', October 20009, see PMG., 'Protection of Personal Information Bill [B9-2009]: public hearings',
http://www.pmg.org.za/report/20091013-protection-personal-information-bill-b9-2009-public-hearings,
last visited 18/04/2012.
1894 Ibid, note 250, supra. An issue paper is the first step in the consultation process. The purpose of an issue paper is to announce an investigation, to elucidate the aim and extent of the investigation, to point to possible options available for solving existing problems and to initiate and stimulate debate on identified issues by way of including specific questions on relevant issues, see South African Law Reform Commission Website,
http://salawreform.justice.gov.za/ipapers.htm lat visited 18/04/2012.
1895 South African Law Reform Commission, Discussion Paper 109, note 249, supra. Discussion papers, previously referred to as working papers, are documents in which the Commission's preliminary research results are contained. In most cases discussion papers also contain draft legislation which gives effect to the Commission's tentative recommendations and proposals. The main purpose of these documents is to test public opinion on solutions identified by the Commission, see South African Law Reform Commission Website,
http://salawreform.justice.gov.za/dpapers.htm last visited 18/04/2012.
1896 South African Law Reform Commission, Project 124, Report, note 253, supra.
1897 Ibid.

Department of Justice and Constitutional Development and SALRC briefed the Committee on the Bill on 6 and 7 October 2009.[1898] One of the issues that was raised by members of the Portfolio Committee was that the SALRC's Report focused on the first world countries such as the USA, Britain; Canada and Australia as best practice. They wanted to know from the Department and SALRC why there was no developing country mentioned in the report with regard to privacy laws. The response by Ms. Louw for the Department was that one should not look at the countries in particular, although one could look at the example of what was happening in other countries. She pointed out that the South African Data Protection Bill was based on international instruments and that is what they had complied with to get the adequacy rating. The examples used were made because the countries mentioned had legislation already. South Africa did not necessarily copy their implementation. It was following the international instruments. She noted that the countries in Africa had only implemented their laws recently. Senegal was the first to implement in 2006. The other three (Morocco, Benin and Burkina Faso) had only adopted their privacy legislation in 2009. They were also following the European Union instruments. As pointed out in 1.2.1 and elsewhere in this thesis, one can note that most of the responses of Ms. Louw regarding the state of privacy legislation in Africa are misleading.

On 13 October 2009, the Portfolio Committee held public hearings.[1899] The Committee received 35 submissions from individuals and organisations. Subsequently, the Portfolio Committee met on eight separate occasions (21, 27 and 28 October 2009; 4 November 2009; 24 February 2010; 2 March 2010; and 8 and 9 April 2010) to deliberate on the Bill.[1900] Since then the Portfolio Committee left the Technical Sub-Committee (TSC) to deal with the Bill and report to it for further deliberations by the full Committee. The TSC had met on eleven separate occasions (21 May 2010; 4 June 2010; 13 August 2010; 15, 16 and 24 February 2011; 1 March 2011; 19 September 2011; 10 October 2011; 7 November 2011 and 29 March 2012).[1901] It is imperative to note that the 29 March 2012 was the last meeting of the TSC.[1902] In this last meeting, it was decided that the seventh working draft of the Bill be submitted to the full Portfolio Committee for deliberations before it is sent back to the Parliament for debate.

[1898] PMG, note 1783, supra; see also, PMG., 'Protection of Personal Information Bill [B9-2009] briefing', 7th October 2009; http://www.pmg.org.za/report/20091007-protection-personal-information-bill-b9-2009-briefing, last visited 19/04/2012.

[1899] PMG., note 1893, supra.

[1900] See PMG, All Committee Reports (Justice and Constitutional Development) from October 2009 to March 2012; PMG Website.

[1901] Ibid.

[1902] PMG., 'Protection of Personal Information Bill [B9-2009] sixth working draft: technical sub-committee deliberations' http://www.pmg.org.za/report/20120329-deliberations-protection-personal-information-bill, last visited 20/04/2012.

6.4.3.3 Urgency for PPIA

With the exception of Van der Merwe, South African commentators are unanimous that the creation of data protection measures through legislation is a matter of great urgency.[1903] Yet for more than decade such urgency has not turned a reality. As alluded to, data protection legislation has been on legislative agenda in South Africa since mid-1990s. However, the last event that accentuated the urgency for the adoption of the data protection legislation, at least from the commentators' point of view, was the 2010 FIFA World Cup which took place in South Africa. It was widely viewed by commentators that the World Cup would have put some sort of pressure on South Africa to pass its pending data privacy Bill 2009 into law. Heyink notes, 'the Protection of Personal Information Bill was urgent in 2002, and now it's even more urgent in 2009, because of the 2010 World Cup.'[1904] This was due to the fact that under Article 25 of the European Directive 95/46/EC South Africa would not qualify as providing adequate level of protection of personal data. Considering that the World Cup was to result into transfer of massive amount of personal information of European citizens to South Africa during that period, Europe would insist on data privacy legislation. To be sure Ms. Alison Tilley, Executive Director of the Open Democracy Advice Centre, posits:-

> 'Eight years later, this legislation is now (sic) finally ready, but this is where the World Cup comes in. European airlines cannot transfer their Advance Passenger Information to SA, unless we have data protection legislation equivalent to that of Europe, which we don't. We require API from these airlines. They can't give it to us without legislative safeguards. You would think the answer to this would be treating the legislation as a top priority. Unfortunately, the legislation is not yet even on its way to the cabinet-the likelihood of it going through Parliament this season is zero.'[1905]

To partly mitigate the mischief and assure Europeans that their personal information during the 2010 FIFA World Cup would not be misused, the South African government amended the Customs and Excise Act 1964[1906] by introducing a new section 7A through the Revenue Laws

---

[1903] Neethling *et al.*, (Neethling's Law of Personality), p.271, note 186, supra.
[1904] IT Web Security., '2010 pressure mounts on privacy Bill', 26 November 2009, http://www.itweb.co.za/index.php?option=com_content&view=article&id=28415:2010-pressure-mounts-on-privacy-bill&catid=69:business&Itemid=58 last visited 20/04/2012.
[1905] Tilley, A., 'Airline Security sets offside trap for World Cup', BusinessDay, 22 September 2008, http://www.businessday.co.za/Articles/Content.aspx?id=53915 last visited 20/04/2012.
[1906] Act No.91 of 1961.

Amendment Act 2008.[1907] This provision became effective on 8 January 2009.[1908] Section 7A regulates personal information in the context of Advance Passenger Information (API). While this provision may fall under Article 26 of the EU Directive 95/46/EC providing exceptions to the general 'adequacy' standard under Article 25, it is doubtful if it really meets any of such conditions. This is because, similar legislation in the United States of America has been subjected into stringent scrutiny by EU organs without successful results.[1909] Some commentators in South Africa such as Tilley have also cast doubt as to the adequacy of section 7A of the Customs and Excise Act 1964.[1910] At the same time it has been suggested by Roos that beyond Advance Passenger Information, South Africa has to use contractual clauses for adequate protection measures for every international commercial transaction that involves the transfer of personal data from overseas to South Africa, such as the selling of tickets for the World Cup games in the names of specific persons.[1911] Similar views are maintained by Ncube positing that South Africa has not been declared as having adequate level of protection of personal data nor has a determination been made regarding the adequacy of contractual clauses. Data may be flowing to South Africa in terms of Article 26(1) of the European Directive 95/46/EC.[1912]

There are several explanations behind the delay for adoption of data privacy law in South Africa despite the urgent call to do so by commentators. It has been argued that despite proposals for the adoption of an Act for the protection of personal information being on the table for more than three years, it seems as if the political will to enact such law is absent.[1913] Moreover the *ad hoc* strategy of adopting section 7A in the Customs and Excise Act 1964 also runs itself the risk of derailing the real data protection legislation, which South Africa needs if it has to have the call centres managing all that European data.[1914] This is because the need of the law somewhat diminishes if there are other options to rely to achieve similar results. Other reasons that may have contributed to the long delay of data protection legislation are heavy costs of implantation on part of government and private sector once the law is enacted. During the deliberations of the Technical Sub-Committee it transpired that the budget of the data processing authority under the Bill which is projected at R 17 million rand (approximately USD 2,179,487) is

[1907] Act No. 61 of 2008.
[1908] South African Government Gazette No. 31782 of 8th January 2009.
[1909] European Council, note 1078, supra.
[1910] Tilley, note 1904, supra.
[1911] Roos (Personal Data Protection in New Zealand), p.98, note 38, supra.
[1912] Ncube, p.19, note 38, supra.
[1913] Roos (Personal Data Protection in New Zealand), p.65, note 38, supra.
[1914] Tilley, note 1905, supra.

inadequate to implement the legislation once enacted.[1915] This has also been the case for the private companies who mostly submitted that the new law should not overburden them with costs of implementation. To be sure, while the Association for Savings and Investment South Africa supported the purpose and objectives of the Bill, it called for a more moderate pace for implementation in order to balance the risks and costs associated with the new regime.[1916] The company submitted that the imposition of the new privacy regime established by the Bill would be a major undertaking and would have a substantial economic impact on companies. This view was shared by many companies including the Business Unity South Africa who submitted that it was important that once enacted into law, the implementation of the Bill was carefully managed so as to minimise the costs to businesses.[1917] Partly because of this, there have been lobbying by businesses to get certain kinds of data processing exempted from the application of the data protection legislation.[1918] As pointed out, some private companies, particularly those engaging in the business of direct marketing have been in strong opposition of the Bill as it threatens their business.[1919]

It can be submitted that a lengthy consultation process for adopting data protection legislation in South Africa reflects the country's historical past in the apartheid regime. This has been the case with other pieces of legislation such as those regulating freedom of information and interception of communications. By their nature of secrecy or interfering with individual's rights, adoption of such laws have been contentious. With respect to the Data Protection Bill, various interests have similarly been operating for and against the adoption of the data privacy legislation. As there is no specific deadline for the adoption of the data privacy Bill, it is not clear when South Africa will pass its data privacy legislation.

6.4.3.4 Scope and Application

The scope of the Bill is broad. It applies to both automatic and non-automatic processing of personal information by a 'responsible party'.[1920] The term 'responsible party' is similarly broadly defined. It means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.[1921] This

[1915] PMG, note 1893, supra.
[1916] Ibid.
[1917] Ibid.
[1918] Ibid.
[1919] Ibid, note 1785, supra.
[1920] Protection of Personal Information Bill 2009, s. 3(1),(a).
[1921] Ibid, s.1.

means that the Bill proposes a law that is applicable to both the public and private sector and above all the individuals. It is interesting to note that in its wider scope the Bill extends its ambit to juristic and non-juristic persons in the private sector. This is because the term 'private body' is interpreted as a natural person who carries on any trade, business or profession; a partnership or juristic person.[1922]

However the Bill has its limitations which may make it falls short of the European Directive 95/46/EC. 'Operator' is defined in the Bill as a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.[1923] This definition is equivalent to 'processor' in Article 2(e) of the Directive. Yet the Bill lacks an equivalent definition of the term 'third party' in Article 2(f) of the Directive who is not a data subject, data controller or processor but someone who processes data under the direct authority of the controller or processor.

The scope of the Bill is also limited by the definition of 'processing'. It is imperative to note that in the original Bill 'processing' is assigned a broad definition similar to the one in Article 2(b) of the European Directive. This has led Roos to observe that 'this definition is so wide that one can argue that "processing" could be any action performed on personal information.'[1924] However in the sixth working draft of the Bill, the Technical Sub-Committee of the Portfolio Committee has proposed a narrow definition of 'processing' as an option to the original definition. The latter states:-

> 'Processing' means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including (a) the collection, receipt, recording (b) dissemination by means of transmission, distribution or making available in any form; or (c) merging, linking, as well as blocking, degrading, erasure or destruction of information; but excludes the collection, storage or updating of blocked information.'[1925]

[1922] Ibid.
[1923] Ibid.
[1924] Roos, p.368, note 201,supra.
[1925] Protection of Personal Information Bill 2009, s. 1, Option 14. 'Blocking' means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information or (Option 3) 'Blocked' as referred to information means information which placed contained in a data bank which-(a) remains unused and inaccessible for as long as it is unused and inaccessible, provided that safeguards are in place to verify whether it is used or accessed, or (b) is kept in a place or in manner which prevent the use of such information as prescribed, see Protection of Personal Information Bill 2009, s. 1.

The above definition omits 'organisation, collection, storage, updating or modification, retrieval, alteration, consultation or use' from the definition of 'processing' in the original definition of the Bill.[1926] Moreover, the proposed new definition excludes certain operations 'collection, storage or updating of blocked information' from the ambit of 'processing'. It can be submitted that the sets of definitions of the term 'processing' are materially different. One cannot equate them by simply picking the expressions 'any operation or activity or any set of operations' and 'including' just before the enumerations of such operations or activities or set of operations in the two definitions. While these expressions suggest broad ambit of the two definitions, it is arguable that the specific exclusion in the proposed new definition leaves no doubt that the new definition intends to limit the scope of the definition of the term 'processing'. If the Bill is finally passed into law with an inclusion of the proposed new definition of 'processing' it is clear that the South African data privacy regime will fall short of the EU law in this context.

Similarly, the narrow definition of 'processing' limits the term 'personal information'. The latter appears in the original Bill as broad.[1927] However in the proposed option, the Sub-Committee has proposed both a broad and narrow definition. In the broad sense, the proposed definition just as it is the original definition, maintains a list of an exhausted list of what amounts to 'personal information' with an addition of one paragraph.[1928] Moreover, it extends the meaning of personal information to both natural and juristic persons as data subject.[1929] Yet, in line with the definition

[1926] The original definition provides that 'processing' means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as blocking, degradation, erasure or destruction of information, see Protection of Personal Information Bill 2009, s. 1.

[1927] 'Personal information 'means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of a person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person; (d) the blood type or any other biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person, see Protection of Personal Information Bill 2009, s. 1.

[1928] A proposed paragraph adds '(i) consumer or purchasing preferences or patterns: Provided that such information is-(i) used or meant to be used in trade or commerce; (ii) not in the public domain in the same or in a different format; or (iii) held by a public body', as part of 'personal information', see Protection of Personal Information Bill 2009, s. 1, Option 12.

[1929] 'Person' means a natural person or a juristic person; and a 'data subject' means the person to whom personal information relates; see Protection of Personal Information Bill 2009, s. 1.

of 'processing' it excludes 'blocked information' from the list of 'personal information'.[1930] Thus it is submitted that the South African data privacy law may not meet the equivalent standard of personal information provided in Article 2(a) of the European Directive.

Furthermore, the application of the Data Protection Bill rests on the 'territoriality principle'. This means that the Bill when becomes law it will apply on the processing of personal data of a responsible party taking place in South Africa. To be sure section 3(1), (b) of the Bill states:-

> '3(1) This Act applies to the processing of personal information (b) where the responsible party is (i) domiciled in the Republic and the information is processed in Republic; or (ii) not domiciled in the Republic, but makes use of automated or non-automated means that are situated in the Republic, unless those means are used only to transfer personal information through the Republic.'

The Bill defines the expression 'automated means' in the above section as any equipment capable of operating automatically in response to instructions given in processing information.[1931] It is imperative to note that while section 3(1)(b) is similar to Article 4 of the European Directive, it omits a requirement that a data controller must designate a representative in the Republic. This may bring difficulties for data subjects to exercise their rights. Moreover it is likely to result in difficulties of enforcement by the data protection authority.

Besides the scope of application of the Bill explained above, it is noteworthy that the proposed law contains an extensive data exemption regime. The provisions of the Bill do not apply when processing personal information in the course of a purely personal or household activity.[1932] It is arguable that any person who keeps a directory of telephone numbers and addresses of friends and acquaintances for personal use processes data for a purely personal or household activity.[1933] Clearly this type of activity ought not to be regulated by legislation, since the risk posed to the privacy activity of third parties is minimal.[1934] The Technical Sub-Committee of the Portfolio Committee has proposed an option provision which excludes the provisions of the Bill from the

[1930] Protection of Personal Information Bill 2009, s. 1, Option 12.
[1931] Ibid, s.3 (4).
[1932] Ibid, s.6(1)(a).
[1933] Roos, p.371, note 201, supra.
[1934] Ibid.

processing 'in the course of non-commercial, non-governmental or household activity'.[1935] This proposed new provision is broader than the EU law, and in particular it may not be compatible with Article 3(2) of the Directive. This is because 'non-commercial and non-governmental' entails a broad range of processing activities which may render the Bill defeats the very purpose of its enactment. Also excluded from the application of the Bill is processing of personal data that has been de-identified to the extent that it can be re-identified again.[1936] 'De-identify' or 'de-identified' in relation to personal information of a data subject, means to delete any information that-(a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.[1937] On the other hand, the Bill defines the terms 're-identify' or 're-identified' in relation to personal information of a data subject, as resurrect any information that has been de-identified, that- identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.[1938] To say the least, this provision is not available in the EU law. Also its implementation will require a maximum level of transparency.

The provisions of the Bill are also excluded from application in respect to processing operations concerning national security, defence, public safety and activities of public bodies in the areas of criminal law, prosecution and execution of sentences.[1939] However this provision puts one caveat: that exclusion is permissible only where respective legislation regulating public bodies in those areas provides 'adequate safeguards' for the protection of such personal information. Section 6(1)(c) of the Bill is equivalent to Article 3(2) of the European Directive. Yet one may argue that it provides somewhat higher standard than Article 3(2) of the Directive because while it purports to exclude public bodies from the application of the privacy legislation it does so only to the extent that there are adequate safeguards for processing personal information. However it is interesting to note that the Technical Sub-Committee has proposed a new option of deleting completely section 6(1)(c) from the Bill.

[1935] Protection of Personal Information Bill 2009, s. 6(1)(a), Option 1.
[1936] Ibid, s.6 (1)(b).
[1937] Ibid, s.1.
[1938] Ibid.
[1939] The specific section provides, the provisions of this Act are excluded when processing of personal information, Section 6(1)(c) by or on behalf of a public body and(i) which involves national security, including activities that are aimed at assisting in the identification of terrorist and related activities, defence or public safety; or (ii) the purpose of which is the prevention , detection, including activities that are aimed at assisting in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information.

The other areas where the provisions of the Act will not apply include processing by any person for the purpose of *bonafide* literary or artistic expression and journalistic purposes ;[1940] by the Cabinet and its committees and the Executive Council of a province;[1941] processing relating to the judicial functions of a court referred to in section 166 of the Constitution;[1942] or to the extent that a responsible party has been exempted from the application of such conditions for the lawful processing of personal information as determined by the Information Regulator, the supervisory authority, in terms of section 37 of the Bill.[1943]

It is submitted that some of the exemptions listed in the preceding paragraph particularly those relating to artistic or literary expressions and journalistic purposes are equivalent to Article 9 of the European Directive 95/46/EC. However, the rest of the exemptions have far reaching consequences to individual personal information. For example, the exemptions of the Cabinet and its committees and the Executive Council of the province leave most of the processing of personal information in the public sphere unregulated. Perhaps the worst of these exemptions relate to the powers of the supervisory authority, the Information Regulator, to exempt from the application of the Act of processing by responsible parties.[1944] It is submitted that, much as most of the criteria in section 37 of the Bill upon which the Information Regulator may exempt responsible parties from compliance to the law even though the processing activities would be in breach of an information protection principle are open ended, the requirement to publish a notice in the *Gazette* for the grant of the exemption is not a sufficient safeguard to check abuse by the Regulator. Instead the notice may only serve as a notification to the public of the fact of the exemption rather than a mechanism to check possible abuse by the Regulator. Moreover, the language of 'may' used in the beginning of section 37 clearly suggests that the publication of notice is not obligatory. The Regulator may not publish it and still be in compliance to the law.

[1940] Protection of Personal Information Bill 2009, ss. 6(1)(d) and 7.
[1941] Ibid, 6(1)(e), with an option to delete the whole paragraph(e).
[1942] Ibid, 6(1)(f).
[1943] Ibid, 6(1)(g).
[1944] Section 37 of the Bill states (1)The Regulator may, by notice in the Gazette, grant an exemption to a responsible party to process personal information, even if that processing is in breach of a condition for the processing of such information if the Regulator is satisfied that, in the circumstances of the case-(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or (b)the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing. (2)The public interest referred to in subsection (1) includes-(a)the interests of national security; (b)the prevention, detection and prosecution of offences; (c)important economic and financial interests of a public body; (d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c); or (e) historical, statistical or research activity. (3) The Regulator may impose reasonable conditions in respect of any exemption granted under subsection (1).

Similarly, the provision of section 37(3) which provides 'the Regulator may impose reasonable conditions in respect of such exemptions' may not guarantee safeguards. It is entirely upon the Regulator to determine which conditions are reasonable in a particular case. Moreover, it is not mandatory to impose any of the so called 'reasonable conditions'. It can be submitted that the whole of chapter 4 of the Bill comprising sections 36 and 37 on exemption from conditions for processing of personal information by the Regulator may not likely satisfy the standards set by the European Directive. Together with other discussed shortcomings, it may negatively impact on the overall assessment of the 'adequacy' standards by the EU organs.

The application of the Bill when becomes law is also limited in relation to other legislation which regulates processing personal information. In the first place, the Bill provides that the Act will generally prevail over any other legislation which is materially inconsistent with an object, or a specific provision, of this Act.[1945] Yet, when such other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in chapter 3, the extensive conditions prevail.[1946] One of likely situations that is envisaged by this second scenario is sector specific laws regulating personal processing.

6.4.3.5 Data Protection Principles

The Data Protection Bill is based on the eight data protection principles. These principles are referred to as conditions for lawful processing of personal information. They are similar to, but not exactly the same as, the principles found in the OECD *Guidelines* and the European Data Protection Directive 95/46/EC.[1947] The Data Protection Bill lists the data protect protection principles in section 5(1)(a)-(h) as accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation respectively. Each of these basic principles is elaborated in details in chapter three of the Bill (sections 8-25). Compared to the original Data Protection Bill, one may find that the sixth working draft of the Bill has introduced some changes on these principles, although not so significant. First, the original Bill numbered the basic principles serially from principles 1 to 8. This is no longer the case in the sixth working draft. The working draft has abandoned such manner of numbering. It is important to note that the abandonment of numbering the basic principles of data protection came right away in the first working draft of the Bill. Part and parcel

[1945] Protection of Personal Information Bill 2009, s. 3(2)(a).
[1946] Ibid, s.3(2)(b).
[1947] Roos, note 1933, supra.

of this shift in the structure of the Bill is a controversial debate among the members of the Technical Sub-Committee in their deliberations of 2 March 2010 and 8 April 2010 whether the Bill was principle or rule based. This debate has never successfully ended. Because of this, the Committee decided to abandon specific reference 'principle' and the corresponding numbering. Similarly, the Committee did not opt to make reference of the principles as 'rules' because the same was confusing. Instead, it introduced section 5(1)(a)-(h) presumably to ease reference of the basic principles to the general public. Second, the sixth working draft of the Bill has re-arranged the basic principles of data processing. Third, the scope and ambit of these principles have either been broadened or narrowed in some cases. Since the sixth working draft of the Bill is a work in progress, this part does not offer definitive detailed discussion.

The first principle of data processing is accountability.[1948] It imposes obligation on a responsible party to comply with conditions of processing set out in chapter 3 of the Bill and all measures that give effect to them. Since the responsible party is usually 'the natural person, juristic person, administrative body or other entity which, which alone or in conjunction with others, determine the purpose of and means for processing personal information', it is clearly the senior person or body in an organisation who will ultimately be held responsible for a breach of the principles by the persons processing the information.[1949] Accountability is an express principle in the EU proposed General Data Protection Regulation. However, it manifests in different principles in the Directive.

The Bill contains processing limitation as the second basic principle of data processing.[1950] The latter provides that personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject unnecessarily. It is important to note that the expression 'unnecessarily' was introduced by the Technical Sub-Committee during its deliberations of 4 June 2010 to highlight the notion that some degree of *prima facie* infringement is permissible. Also important to note is that the principle of processing limitation is a composite of four other sub-requirements. First and foremost is the requirement of lawful processing. This simply means there must be in existence some sort of legal basis for processing personal data. It also entails some balancing of the rights of the data subjects against data processing. The second sub-requirement is minimality.[1951] It aims to limit the amount of personal information collected

[1948] Protection of Personal Information Bill 2009, s. 8.
[1949] Roos, p.380, note 201, supra.
[1950] Protection of Personal Information Bill 2009, s. 9.
[1951] Ibid, s.10. The Technical Sub-Committee has proposed an option provision which states 'Unless authorised under the law or objectively necessary for the completion of the transaction concerned, no-one shall be required to

only to what is necessary to achieve the purpose(s) for which the information is processed.[1952] This is regardless of the lawfulness of the processing itself. Hence the minimality sub-principle requires that only adequate, relevant and in excessive personal information should be processed. The third requirement appears as consent, justification and objection.[1953] These are collectively referred in Article 7 of the EU Directive as conditions for processing. To be sure section 11 states:-

> '11. (1) Personal information may only be processed if-
>
> (a) the data subject or a competent person where the data subject is a child consents to the processing; (b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; (c) processing complies with an obligation imposed by law on the responsible party; (d) processing protects a legitimate interest of the data subject; (e) processing is necessary for the proper performance of a public law duty by a public body; or (f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.'

Section 11 provides further that the data subject may object on reasonable grounds his or her personal data to be subjected into processing by the responsible party.[1954] Once the data subject has objected the processing, the responsible party may not proceed with the processing of his or her personal information.

The fourth sub-requirement of the processing limitation is called 'collection directly from data subject'.[1955] The latter provides that except with some specified situations, the responsible party must collect personal information directly from the data subject.[1956] This requirement is not laid

---

provide or disclose personal information as a condition for the completion of a transaction or the receipt of a benefit', see Option 31.

[1952] Roos, p.372, note 201, supra.

[1953] Protection of Personal Information Bill 2009, s. 11.

[1954] Section 11(2) A data subject may object, at any time, on reasonable grounds relating to his, her or its particular situation, in the prescribed manner, to the processing of personal information in terms of subsection (1)(d) to (f), unless legislation provides for such processing. (3) If a data subject has objected to the processing of personal information in terms of subsection (2), the responsible party may no longer process the personal information.

[1955] Protection of Personal Information Bill 2009, s. 12.

[1956] Section 12 of the Data Protection Bill states, 12. (1) Personal information must be collected directly from the data subject, except as otherwise provided for in subsection (2). (2) It is not necessary to comply with subsection (1) if- (a) the information is contained in or derived from a public record or has deliberately been made public by the data subject; (b) the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source; (c) collection of the information from another source would not

down in the 1995 Data Protection Directive and at the first glance may seem unnecessarily strict.[1957] Yet, it may be implied in Articles 10 and 11 of the EU Directive which require the data controller to supply certain information when personal data are collected from the data subject directly or indirectly respectively.

The third principle of data protection is the purpose specification.[1958] According to this principle, personal information must be collected for a specific, explicitly and lawful purpose related to a function or activity of the responsible party.[1959] The responsible party must always ensure that the data subject is aware of the purpose of the collection of the personal information unless provided in section 18(2) of the Act.[1960] The purpose specification principle also requires that records of personal information must not be retained any longer than is necessary for achieving the purpose for which information was collected or subsequently processed.[1961] However, there are exceptions to this general principle where retention of the record is required or authorised by law; the responsible party reasonably requires the record for lawful purposes related to its functions or activities; retention of the record is required by a contract between the parties thereto; or the data subject or a competent person where the data subject is a child has consented to the retention of the record.[1962] It is imperative to note that the Technical Sub-Committee has proposed three options with respect to data retention which may significantly detract from the conditions of data processing in chapter 3 of the Bill.[1963]

The fourth principle of data processing is further processing limitation.[1964] Usually, the further processing of information is dealt with as part of the purpose limitation principle.[1965] However, it

---

prejudice a legitimate interest of the data subject; (d) collection of the information from another source is necessary- (i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences; (ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997); (iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; (iv) in the interests of national security; or (v) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied; (e) compliance would prejudice a lawful purpose of the collection; or (f) compliance is not reasonably practicable in the circumstances of the particular case. (g) the information- (i) is or is placed in a data bank operating in terms of a code of conduct; or (ii) is transferred from a data bank operating in terms of a code of conduct to another data bank or entity operating in terms of a code of conduct.

[1957] Roos, p.373, note 201, supra.

[1958] Protection of Personal Information Bill 2009, s. 13.

[1959] Ibid, s.13(1).

[1960] Ibid, s.13(2).

[1961] Ibid, s.14(1).

[1962] Ibid, s.14 (1)(a)-(d).

[1963] Ibid, Options 38,39 and 40.

[1964] Ibid, s.15.

[1965] Roos, p.376, note 201, supra.

has been made to stand as an independent principle in order to emphasise its importance.[1966] The further processing principle prohibits processing of personal information in a way that is incompatible with the purpose of its original collection.[1967] The assessment of compatibility must take into account: the relationship between the purpose of the intended further processing and the purpose for which the information has been collected; the nature of the information concerned; the consequences of the intended further processing for the data subject; the manner in which the information has been collected; and any contractual rights and obligations between the parties.[1968] The Bill provides specific exceptions where processing must not be regarded as incompatible to the original purpose(s).[1969]

Information quality constitutes the fifth data protection principle under the Bill.[1970] It states that the responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.[1971] There are no exceptions to this principle. This partly suggests that every responsible party has no option other than compliance. However, there are some challenges in implementation of this principle. For example, the responsible party may for purposes of safeguarding his or her interest deliberately omit to take 'reasonably practicable steps' envisaged under this principle. Roos illustrates this situation clearly. She observes that if the responsible party records the fact that the data subject refused to pay for a product or service, but does not record that the data subject refused to pay because he or she was dissatisfied with the service or product, the information is incomplete and therefore misleading.[1972] The impression created by information should not be misleading and should give a complete picture of the data subject's situation.[1973]

1966 Ibid.

1967 Protection of Personal Information Bill 2009, s. 15(1).

1968 Ibid, s.15 (2)(a)-(e).

1969 Section 15 of the Data Protection Bill states, (3)The further processing of personal information is not incompatible with the purpose of collection if-(a)the data subject or a competent person where the data subject is a child has consented to the further processing of the information;(b)the information is available in or derived from a public record or has deliberately been made public by the data subject;(c)further processing is necessary-(i)to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;(ii)to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);(iii)for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or(iv)in the interests of national security;(d)the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to-(i)public health or public safety; or(ii)the life or health of the data subject or another individual;(e)the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identified form; or (f)the further processing of the information is in accordance with an authority granted under section.

1970 Protection of Personal Information Bill 2009, s. 16.

1971 Ibid, s.16 (1).

1972 Roos, p.377, note 201, supra.

1973 Ibid.

The expression 'reasonably practicable steps' used in the formulation of the information quality principle clearly suggests that total accuracy is not absolutely guaranteed.[1974] Likewise the necessity of updating information is determined by the purpose for which the information is held.[1975] For example, updating is unnecessary if information is part of a historical record, but is necessary if it is used for a purpose such as credit rating.[1976]

The sixth data protection principle is openness.[1977] This principle requires the responsible party to notify both the Regulator and the data subject of the planed data processing.[1978] With regard to notification to the Regulator, the detailed provisions of chapter 6 of the Bill should be adhered to. This type of notification has to be noted in the register kept by the Regulator.[1979] However, in case of the data subject, the responsible party is required to supply a set of information before processing takes place or as soon as reasonably practicable after it has been collected.[1980] Such information include the information being collected; the name and address of the responsible party; the purpose for which the information is being collected; whether or not the supply of the information by that data subject is voluntary or mandatory; the consequences of failure to provide the information; any particular law authorising or requiring the collection of the information; and any further information such as the-recipient or category of recipients of the information; nature or category of the information; existence of the right of access to and the right to rectify the information collected; and the existence of the right to object to the processing of personal information.[1981] However, the requirement of notification is not absolute. It has a wide range of exceptions.[1982]

The seventh principle is security safeguards.[1983] By this principle, a responsible party must ensure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information an unlawful access to or processing of personal information.[1984] The Bill lists specific measures that have to be taken by the responsible party to give effect to the requirement security safeguards: to identify all reasonably foreseeable

[1974] Ibid.
[1975] Ibid.
[1976] Ibid.
[1977] Protection of Personal Information Bill 2009, s. 17.
[1978] Ibid, ss.17 and 18.
[1979] Ibid, s.60.
[1980] Ibid, ss.18 (2)(a) and (b).
[1981] Ibid, s.18(1)(a)-(g).
[1982] Ibid, ss. 18(3),(4); and 59.
[1983] Ibid, s.19.
[1984] Ibid, s.19 (1).

internal and external risks to personal information in its possession or under its control; establish and maintain appropriate safeguards against the risks identified; regularly verify that the safeguards are effectively implemented; and ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.[1985] Moreover, the security principle requires that the responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.[1986]

It is imperative to note that the security safeguards principle does not bind the responsible party only. It extends to an operator and anyone who processes personal information on behalf of a responsible party or operator.[1987] In this kind of situation, processing of personal information is only permitted with the knowledge or authorisation of the responsible party.[1988] Moreover, such information must be treated as confidential and must not be disclosed unless required by law or in the course of the proper performance of their duties.[1989] To ensure that those measures are adhered to by the operator or any other person, the processing of personal information by the operator or such other person must be governed by written contract.[1990] It can be submitted that the Data Protection Bill somewhat corresponds to the safeguards in the EU Directive when it comes to security safeguards in the context of processing by 'operators' and 'anyone processing personal information on behalf of a responsible party or an operator'. This is because; Article 17(3) of the Directive provides categorically that processing by way of a 'processor' must be governed by a contract or legal act binding the processor to the controller. Moreover, for purposes of keeping proof, Article 17(4) of the Directive obliges that the paries of the contract or the legal act relating to data protection and the requirements relating to security measures must be in writing or in another equivalent form. Yet, the Directive is somewhat broader in two senses. First, the expression 'legal act' leaves other possibilities other than the use of 'contract' to bind the processor with the terms of security measures. Second, the expression 'in another equivalent form' leaves other possibilities of keeping proof other than the use of 'writing'. In the present age of extensive use of ICTs where electronic contracts are legally recognised and are enforceable, the EU law makes perfect a sense as compared to what the Data Protection Bill

[1985] Ibid, s.19(2).
[1986] Ibid, s.19(3).
[1987] Ibid, s.20.
[1988] Ibid, s.20 (a).
[1989] Ibid, s.20 (b).
[1990] Ibid, s.21(2).

provides. The Bill also has provisions which the responsible party has to comply whenever there are breaches of security safeguards.[1991]

The eighth data protection principle is the data subject participation.[1992] Usually the data subject participation principle entails a bundle of rights that may be exercised by the data subject in relation to his or her personal information. These include a right of access to his or her personal information, a right of correction of inaccurate information and a right to object the processing of personal information in certain situations, for example in direct marketing.[1993] However, in its earlier working drafts of the Bill, only two rights were provided: the right of access and the right to request correction.[1994] The sixth working draft of the Bill has expanded the horizon of the data subject participation principle. The draft has incorporated a new section 4 titled 'rights of the data subjects'.[1995] The rights included in section 4 of the Bill are: right to object processing; right to be notified processing; request of confirmation of processing; correction, destruction and deletion; right to refuse to participate in direct marketing; right to refuse to be subjected to a decision based solely on the basis of the automated processing; right to submit complaint to the Regulator; and right to institute civil proceedings regarding interference of his or her personal information. It can be submitted that section 4 of the Bill is generally a pointer of specific rights scattered in the Bill to ease their attention to the public. However, in order to exercise these rights the data subject must over and above rely specifically to the provisions pointed out under

[1991] Ibid, s.22.
[1992] Ibid, s.23.
[1993] Roos, p.379, note 201, supra.
[1994] Ibid.
[1995] Section 4 of the data Protection Bill provides: 4. A data subject has the right to have his, her or its personal information processed by or for a responsible party in accordance with the conditions for the lawful processing of personal information as referred to in section 5, including the right- (a) to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11; (b) to be notified that- (i) personal information about him, her or it is being collected as provided for in terms of section 18; or (ii) his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22; (c) to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23; (d) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24; (e) to refuse the processing of his, her or its personal information for the purpose of direct marketing by means of unsolicited electronic communications as provided for in terms of section 74; (f) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 76; (g) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 79; and (h) to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 102.

section 4. It is also important to note that the data subjects' rights are not absolute. There are some limitations on them.[1996] These must be adhered to by the data subjects.

The regime of international transfer of data is also provided in the Data Protection Bill.[1997] This regime provides that a responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country.[1998] However, personal data may be transferred where the recipient of the information is subject to a law, binding code of conduct or binding agreement.[1999] These instruments must effectively uphold principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information; and include provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country.[2000] The other exception is where the data subject consents to the transfer; the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or the transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject to that transfer; and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.[2001] It is submitted that the South African proposed international regime of data transfer may not meet the standard of the EU law. This is because, the default rule under the EU Directive is provided in Article 25 that data may be transferred to the third country which provides 'adequate' level of protection of personal data. By way of exception, Article 26 of the Directive provides that data may still be transferred to a third country which does not provide 'adequate level' of protection of personal data. Surprisingly, the South African Bill does not in the first place restrict transfer of personal data to a foreign country just as it is the case with Article 25. Instead, the Bill picks Article 26 of the Directive and makes it the default rule. While section 77 of the Data Protection Bill can be said to provide minimum fulfilment of the requirement of the European law, it is doubtful if it may be accepted by Europe. This doubt is exacerbated by the fact that similar approach elsewhere,

[1996] Most of the limitations for the exercise of the data subjects' rights are provided in specific provisions scattering in the Data Protection Bill.
[1997] Protection of Personal Information Bill 2009, s. 77.
[1998] Ibid.
[1999] Ibid, s.77(a).
[2000] Ibid,s.77(a)(i)-(ii).
[2001] Ibid, s.77(b)-(e).

particularly the APEC data privacy framework has been considered by Europe as a weak standard.

Apart from the eight data protection principles, the Data Protection Bill incorporates principles for processing special categories of personal information. There are four main categories of this class of personal information and their corresponding principles. The first of them is processing of sensitive personal information. Section 26 provides, 'a responsible party may not process personal information concerning-(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, DNA or sexual life of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relate to-(i) the commission or alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence committed or allegedly committed by a data subject, the disposal of such proceedings or any sentence that has been imposed by a court in such proceedings. It is important to note that the restriction imposed in processing personal data in section 26 of the Bill is subject to both the general and specific exemptions. The general exemptions exclude the application of section 26 where processing is carried out with the consent of a data subject; processing is necessary for the establishment, exercise or defence of a right or obligation in law; processing is necessary to comply with an obligation of international public law; processing is for historical, statistical or research purposes; the data subject has deliberately made his or her individual personal information public; or upon exemption by the Regulator.[2002] The specific exemptions apply to various aspects of sensitive information listed in section 26 of the Bill. These include religious or philosophical beliefs;[2003] race or ethnic origin;[2004] trade union membership;[2005] political persuasion;[2006] health;[2007] criminal behaviour;[2008] and sexual life.[2009] While it is too early to evaluate the provisions of sensitive processing of personal information, it is doubtful if the dual approach of exemptions in the Data Protection Bill may satisfy the standards of the European Directive which incorporates only the general exemptions but not the specific ones as the Bill.

[2002] Ibid, s. 27(a)-(f).
[2003] Ibid, s.28.
[2004] Ibid, s.29.
[2005] Ibid, s.30.
[2006] Ibid, s.31.
[2007] Ibid,s.32.
[2008] Ibid,s.33.
[2009] Ibid, s.33A.

The second category of special processing relates to the processing of personal information of children. The Bill prohibits a responsible party from processing personal information concerning a child.[2010] A 'child' is defined as a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.[2011] However the Technical Sub-Committee has proposed an optional definition which defines a 'child' as a natural person under the age of 13 years.[2012] The processing of personal information of a child is still permissible if the processing is carried out with the prior consent of a competent person; if the processing is necessary for the establishment, exercise or defence of a right or obligation in law; if the processing is necessary to comply with an obligation of the public international law; if the processing is for historical, statistical or research purposes; or exempted by the Regulator.[2013] It is interesting to note that the EU Directive does not contain special provisions governing the processing of a child's personal information. To this extent, the Bill proposes a stronger protection to a vulnerable category of persons.

The third category of processing of personal information in specific contexts is direct marketing. Generally the Data Protection Bill prohibits processing of personal information of a data subject for direct marketing.[2014] The means prohibited are of any form of electronic communication, including automatic calling machine, facsimile machine, SMSs or e-mail.[2015] However, processing of personal information for direct marketing is permitted in certain circumstances. The Bill provides two main exceptions. First, is where the data subject has given his, her or its consent to the processing.[2016] The responsible party may approach the data subject only once in order to obtain consent of the data subject in processing.[2017] The second situation permitting direct marketing is where the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service; for the purpose of direct marketing of the responsible party's own similar products or service; and if the data subject has been given a reasonable opportunity to object the processing of information, free of charge and in a manner free of unnecessary formality.[2018] The Bill provides further that in any communication for the purpose of direct marketing, details of the identity of the sender or the person on whose behalf

[2010] Ibid, s.34.
[2011] Ibid, s.1.
[2012] Ibid, s.1, Option 5.
[2013] Ibid, s.35.
[2014] Ibid, s.74 (1).
[2015] Ibid.
[2016] Ibid, s.74(1)(a).
[2017] Ibid, s.74(2).
[2018] Ibid, ss.74(1) and 74(3).

the communication has been sent; and an address or other contact details to which the recipient may send a request that such communication cease.[2019] There are also special provisions for data processing with respect to directories.[2020] It can be noted that with the exception of directories, the provisions of the Bill on direct marketing are restrictive to electronic communications only. This may leave other forms of direct marketing such as those through post, etc to remain outside the ambit of the law.

The fourth category of special processing is automated decision making.[2021] The Bill incorporates an equivalent provision to Article 15 of the EU Directive on automated decision making. Section 76(1) of the Bill states that a data subject has the right not to be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability and conduct. However automated decision making may be allowed in exceptional circumstances.[2022]

6.4.3.6 Data Protection Commission

For purposes of implementing the data privacy legislation once enacted, the Data Protection Bill provides for the establishment of a data protection authority by the name of Information Regulator (or Regulator).[2023] The Regulator is a juristic person. [2024] It is independent and is subject only to the Constitution and to the law.[2025] In which case, it is required to act impartially and performs its functions and exercises its powers without fear, favour or prejudice.[2026] However, the Regulator is accountable to the National Assembly.[2027] Geographically, the jurisdiction of the

[2019] Ibid, s.74(4).
[2020] Ibid, s.75.
[2021] Ibid, s.76.
[2022] Where the decision-(a) has been taken in connection with the conclusion or execution of a contract, and (i)the request of the data subject in terms of the contract has been met; or(ii)appropriate measures have been taken to protect the data subject's legitimate interests; or(b)is governed by a law or code in which appropriate measures are specified for protecting the legitimate interests of data subjects.(3)The appropriate measures, referred to in subsection (2)(a)(ii), must- (a) provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and (b) require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of paragraph (a); see Protection of Personal Information Bill 2009, s. 76(2).
[2023] Protection of Personal Information Bill 2009, s. 38.
[2024] Ibid.
[2025] Ibid, s.38 (b).
[2026] Ibid.
[2027] Ibid, s.38(d).

Regulator extends throughout the Republic of South Africa.[2028] In terms of exercise of functions and powers, the Regulator has jurisdiction over two statutes: the Data Protection Bill once it becomes law and the Promotion of Access to Information Act 2000 (PAIA).[2029]

The Regulator is composed of chairperson and four ordinary members.[2030] One of the members must be appointed on account of being a practising advocate or attorney or a professor of law at a university.[2031] The rest of the members may be appointed on account of any other expertise and experience relating to the objects of the Regulator.[2032] Members of the Regulator are appointed by the President upon recommendation of the National Assembly.[2033] The chairperson of the Regulator is appointed in a full-time capacity.[2034] Similarly two of the ordinary members of the Regulator must be appointed on a full-time capacity,[2035] while the other two members may be appointed in a full-time or part-time capacity.[2036] With the exception of members appointed in part-time capacity, the rest of members of the Regulator are not permitted to perform any other remunerative work.[2037] Yet, members appointed in full-time capacity may still perform any other remunerative work with the permission of Minister.[2038] The term of office of the members of the Regulator is not more than five years with an eligibility of re-appointment.[2039] During this tenure a member of the Regulator may be removed from office only on the ground of misconduct, incapacity or incompetence; a finding to that effect by a committee of the National Assembly; and by the adoption by the National Assembly of a resolution calling for that person's removal from office.[2040] Such a resolution must be supported by a majority vote of the members of the National Assembly.[2041] Moreover, any person including members of the Regulator who acts on behalf or under the direction of the Regulator is not civilly or criminally liable for anything done in good faith with respect to the exercise of functions or powers under the Data Protection Act or PAIA.[2042] Members of the Regulator are always required to disclose conflict of interests in

[2028] Ibid, s.38 (a).
[2029] Ibid, s.38(c).
[2030] Ibid, s.40(1)(a).
[2031] Ibid, s.40(1)(b)(i).
[2032] Ibid, s.40(1)(b)(ii).
[2033] Ibid, s.40(2).
[2034] Ibid, s.40(1)(c).
[2035] Ibid, s.40(1)(d)(i).
[2036] Ibid, s.40(1)(d)(ii).
[2037] Ibid, ss.40(1)(c) and 40(1)(e).
[2038] Ibid, s.40(4).
[2039] Ibid, s.40(3).
[2040] Ibid, s.40(6)(a)(i)-(iii).
[2041] Ibid, s.40(6)(b).
[2042] Ibid, s.53.

their duties.[2043] They are also under duty of confidentiality not to disclose any information accrued in their duties.[2044] Moreover the remunerations, allowances, benefits and privileges of members of the Regulator are statutorily provided.[2045]

In order to ensure smooth discharge of its duties and powers, the Regulator receives its funds from the sums of money that Parliament appropriates annually, for the use of the Regulator.[2046] The other source is prescribed fees collected by the Regulator.

The Bill provides extensive list of powers, duties and functions of the Regulator.[2047] These are typical of most data protection authorities. They include, for example, to educate the public; to monitor and enforce compliance; make consultations with public on matters affecting them; to handle complaints; to conduct research and report to the Parliament; to issue codes of conduct, to register responsible parties, etc.[2048]

As pointed out, one of the functions and powers of the Regulator is to receive complaints and decide them.[2049] An aggrieved complainant has a right to appeal to the High Court against the decision of the Regulator.[2050] Also a responsible party who is aggrieved by an enforcement notice by the Regulator may appeal to the High Court.[2051] Moreover, the Data Protection Bill provides for civil remedies.[2052] A data subject or at the request of the data subject, the Regulator may institute a civil action for damages in a court having jurisdiction against a responsible party.[2053] A complaint for breach of personal information may also be settled by the parties.[2054] The Bill also creates offences most of them 'procedural' in the sense that they relate to the failure to comply with certain provisions of the Bill.[2055] These offences attract fines and/or imprisonment.[2056] It is

[2043] Ibid, s.44.
[2044] Ibid, s.54.
[2045] Ibid,s.45.
[2046] Ibid,s.52.
[2047] Ibid, s.39.
[2048] Ibid.
[2049] Ibid,s.79.
[2050] Ibid, s.100 (2).
[2051] Ibid,s.100(1).
[2052] Ibid, s.102.
[2053] Ibid,s.102(1).
[2054] Ibid,s.85.
[2055] Ibid, chapter 11.
[2056] Ibid.

interesting to note that the Technical Sub-Committee has proposed what is called 'administrative fines'.[2057]

A preliminary evaluation of the Regulator reveals that it is strongly protected in discharging its duties, functions and powers. It qualifies at least on theory to be an independent supervisory authority. However, since the implementation of the Act depends on other instruments such as regulations and codes of conduct, it is premature at present to provide a thorough assessment of the Regulator. Much will depend on the practice as theory is one thing yet its enforcement is another. Also significant to note, is the fact that the Bill is still a work in progress with alternative options proposed by the Technical Sub-Committee.

6.4.4 EU-Accreditation Process

The South African government has not openly declared its intention to apply for 'adequacy' to the EU.[2058] However there are clear indications that South Africa will seek adequacy rating from the European Union. This is because, one of the reason advanced in the *travaux préparatoires* for the adoption of the data privacy law in South Africa is to comply with the international standards particularly the European Directive.[2059] The strong intention to apply for the 'adequacy' rating from the European Union is similarly demonstrated by the fact that the legislative process of the South African Bill has been predominated by Directive 95/46/EC as its primary reference point. In the last meeting of the Technical Sub-Committee held on 29 March 2012, it was strongly brought to the attention of the Committee that the EU Directive which provided the reference point for the South African Bill was undergoing major reforms.[2060] Based on the European legal developments, it was suggested by Ms Ananda Louw, the Principal State Law Advisor, of the South African Law Reform Commission that the South African data privacy legislation would be enacted sometime in 2014 or 2015, the same time the EU new regime of data privacy may be coming into force.[2061] It is submitted that, since the EU Directive is undergoing reform it may delay the South African legislative process if it waits and see the direction of the new law.

[2057] Ibid, Option 110.
[2058] Ncube, p.346, note 11, supra.
[2059] Portfolio Committee on Justice and Constitutional Development, notes 1847, 1855 and 1856, supra.
[2060] PMG., 'Protection of Personal Information Bill [B9-2009] sixth working draft: technical sub-committee deliberations',
http://www.pmg.org.za/report/20120329-deliberations-protection-personal-information-bill,
last visited 22/04/2012.
[2061] Ibid.

6.4.5 Other Legislation

Currently there are three important pieces of legislation in South Africa which, to certain extent, regulate personal information: the Promotion of Access to Information Act 2000(PAIA),[2062] the Electronic Communications and Transactions Act 2002(ECTA)[2063] and the Regulation of Interception of Communications and Provision of Communication Related Information Act 2002(RICA).[2064] As alluded to, the scope of application of these pieces of legislation is limited. PAIA, for example, is essentially a freedom of information Act. It was enacted to give effect to section 32 of the Constitution 1996. Although it applies on both public and private bodies, it narrowly touches upon processing of personal information. That is, when access of information is sought but not in any other context. This legislation will be administered by the Regulator if the Data Protection Bill is enacted into law without changes in this aspect. ECTA as its name suggests essentially deals with electronic transaction. Its scope on protection of personal data is marginal. RICA regulates interception of communications. The Act's application in the context of processing of personal data is limited in interception. Beyond this, RICA has nothing to regulate.

It is important to note that section 112 of the Data Protection Bill and the Schedule makes substantial amendments to PAIA. Part and parcel of these amendments is the harmonisation of its administration by the Information Regulator. ECTA has few amendments resulted by the Bill. Most of them relate to basic concepts. RICA has not been amended. As pointed out, these pieces of legislation exist side-by-side with the Data Protection Act when the Bill becomes law. However their application is subject to the provisions of section 3(2)(a) and 3(2)(b) of the Data Protection Bill.[2065]

6.5 Conclusion

Concerns for privacy are relatively high in South Africa. One of the catalysts that influences such concerns is the past injustice of the apartheid regime. Although apartheid regime formally ended in 1994, the traumas created by it are still in fresh memories of those who suffered under the system. Perhaps because of this background, privacy has long been protected in South Africa

[2062] Act No.2 of 2000.
[2063] Act No.25 of 2002.
[2064] Act No. 70 of 2002.
[2065] The application of other statutes in relation to the Data Protection Bill has been considered in 6.4.3.4, supra.

through the common law of *delict*. It is imperative to note that *O'Keeffe,* decided in 1954, was the first landmark case on privacy in South Africa. Since that moment privacy claims have become common in South African courts. The impetus to privacy protection came about in 1994 after the constitutional recognition of the right to privacy in the South African Interim Constitution. The same was incorporated in section 14 of the 1996 Constitution which is still applicable to date. Yet the rise of modern technology has rendered the South African common law of *delict* and the constitutional protection of privacy incapable of sufficient protection. Hence the need for comprehensive data privacy legislation came about. However, this has been compounded by strong pressure from the European Union through Articles 25 and 26 of Directive 95/46/EC for non-EU countries to enact data privacy legislation that would be considered 'adequate' by EU. To say the least, compliance to the EU Directive has been the dominant agenda behind the adoption of data privacy legislation solely to secure investments from Europe and participate in international trade. It has also been shown that collectivist culture in its manifestation of *Ubuntu* has no or has insignificant role to influence the privacy concerns and the adoption of privacy legislation. Also to note, the lengthy legislative process of the data privacy legislation in South Africa is explained in the context of contesting interests.

7. Data Protection in Tanzania

7.1 Introduction

Tanzania has neither data privacy legislation nor a Bill on such law. In 2005-2006 the country made an attempt to introduce data privacy legislation through the Bill for the Freedom of Information Act 2006. However, the Draft Bill of this Act did not actually reach the Parliament. Its discussion was ended by the government when it reached its fourth version, that is, Draft No.4. Yet, besides this attempt, Tanzania protects privacy through its Constitution, statutory means and to some marginal extent the common law. This chapter analyses the Tanzania's system of data privacy protection. The latter is situated upon the country's socio-economic and political context. Competing interests around the development of data privacy law are pinpointed and considered as well.

7.2 Socio-Economic and Political Context

Tanzania is a United Republic of the defunct sovereign state called Tanganyika (now mainland Tanzania) and Zanzibar. The two entities united on 26 April 1964. The Union resulted into two governments, the government of the United Republic of Tanzania and the Revolutionary Government of Zanzibar. The government of the United Republic of Tanzania has dual mandates. It caters for union matters between mainland Tanzania and Zanzibar. The United Republic also caters for non-union matters for mainland Tanzania. On the other hand, the 26 April 1964 Union did not extinguish the Zanzibar's sovereignty. It retained a limited sovereignty. Through this, the Revolutionary Government of Zanzibar caters for non-union matters for Zanzibaris. It is important to note that sometimes reference to Tanzania is restrictive of mainland Tanzania but sometimes inclusive of Zanzibar under the Union. In this part, both references are used and are only differentiated by their specific contexts.

Tanganyika gained its independence on 9 December 1961 from the British. However, after the Berlin Conference of 1884-85, it was under the German colonial rule. The German domination ended with their defeat in the First World War (1914-1918). Subsequently, Tanganyika was put under the British as a Trusteeship territory within the mandate of the League of Nations and later the United Nations after the end of the Second World War (1939-1945). However, prior to the German and British rule, Tanganyika had external trade contacts with the Middle and Far

East. These had resulted into Arab and Islamic cultures on local communities living along the coastal areas of the Indian Ocean.

In 1962 Tanzania became a Republic.[2066] This ended Her majesty the Queen of England's post as the head of the government of Tanganyika.[2067] From this moment to date the president has become both the head of state and government. Following the union between Tanganyika and Zanzibar, Tanzania adopted the Interim Constitution of Tanzania 1965. This was replaced by the permanent constitution of Tanzania in 1977, the Constitution of the United Republic of Tanzania 1977(URT Constitution). Since then, the URT Constitution has been amended from time to time to accommodate political, social and economic changes taking place locally and globally. Currently, Tanzania is reviewing its URT Constitution by overhauling it with a new one. The constitutional reform process started last year with the adoption by the Parliament of the United Republic of Tanzania of the Constitutional Review Act 2011.[2068] It is projected that by 2014 Tanzania will have a new Constitution.

On the other hand, Zanzibar was under the Arab domination for centuries. However, during colonisation of Africa, it was put under the British rule. She got her independence from the British on 10 December 1963. This was considered as Arab independence. As a result on 12 January 1964, the Zanzibar Revolution broke out with the overthrow of the Arab government. Since that moment, the government of Zanzibar is called the Revolutionary Government of Zanzibar (RGZ) in order to preserve this historical event.

Compared to Zanzibar, mainland Tanzania has a larger size and population. Located in East Africa, the mainland has a size of about 947,300 square kilometres of which 61,500 square kilometres is inland waters. It is neighboured to the north by Uganda and Kenya; to the east by the Indian Ocean; to the South by Malawi and Mozambique; to the west by Rwanda, Burundi and Zambia. The population in Tanzania is estimated at 43,601,796(including Zanzibar whose population is approximated at 1.2 million) with a large population of about 80% living in rural areas.[2069] However, in large cities like Dar es Salaam, there is rapid urbanisation rate. It is estimated that by 2020 Dar es Salaam will be one of the Africa's megacities in terms of

[2066] The Constitution of Tanganyika 1962, Art 1.
[2067] The Constitution of Tanganyika 1961, Art 11.
[2068] Act No.8Eng of 2011 or Act No.8Sw of 2011.
[2069] CIA World Factbook 2012, http://www.theodora.com/wfbcurrent/tanzania/tanzania_people.html, last visited 25/04/2012.

population.[2070] On the other hand, Zanzibar comprises of the two main Islands of Pemba and Unguja off the east coast of Africa in the Indian Ocean, about 40 kilometres from the port of Dar es Salaam. Its total area is approximately 2,460 square kilometres.

The dominant ethnic group in Tanzania is African. In mainland Tanzania there is about 99% of African (of which 95% are *Bantu* consisting of about 130 tribes) and 1 % the rest of ethnic groups (Asians, European and Arab).[2071] In Zanzibar, there are Shirazi (60%), although black, they distinguish themselves from African; African (35%), Arab, Indians, and Zanzibaris of mixed race (5%).[2072]

Tanzania is a secular state.[2073] Yet, the major religions in Tanzania are Christianity and Islam. There are also other smaller religions existing side-by-side with Christianity and Islam. Although there are no official statistics as to the distribution of the major religions, it is estimated that they are almost the same in number. Yet, in Zanzibar Islam is dominant. Despite ethnic, religious and language diversities, Tanzanians exhibit high level of national identity and low level of ethnic consciousness.[2074] In most cases Tanzanians define themselves in terms of occupation rather than tribe, language or religion.[2075] This is largely attributed to the post-independence measures employed by nationalist leaders to achieve national unity. One of such measures was to promote Kiswahili as the national language. According to the survey by Afrobarometer, just under half of all Tanzanians consider Kiswahili as their 'home language', and it is undoubtedly the *lingua franca* of the majority of citizens.[2076] Through Kiswahili, Tanzanians have created strong social cohesion. It is imperative to point out that English is the second official language.[2077] However it is spoken largely by the country's elite. Moreover, it is used in secondary school, colleges and universities as medium of instruction. It is also used as the language of record of courts except in primary courts and some tribunals. English is also a language of commerce.

[2070] African Business, note 1146,supra.
[2071] CIA World Factbook 2012.
[2072] Notholt, S.A.,'Fields of Fire: An Atlas of Ethnic Conflict' paragraph 2.52, http://books.google.de/books?id=qiKl5jiwp8EC&pg=SA2-PA52&lpg=SA2-PA52&dq=population+ethnic+in+zanzibar&source=bl&ots=3ocDOG7QHk&sig=CYOKTY0lUfI2fbSU2BZ9rdPmhQE&hl=de&sa=X&ei=H26XT6qRLYfysgb7jPW4AQ&ved=0CEEQ6AEwAg#v=onepage&q=population%20ethnic%20in%20zanzibar&f=false last visited 25/04/2012.
[2073] URT Constitution 1977, Art 3.
[2074] Chaligha, A *et al*., 'Uncritical Citizens or Patient Trustees? Tanzanians' Views of Political and Economic Reform' Afrobarometer Paper No.18, 2002, p.2.
[2075] Ibid.
[2076] Ibid, p.8.
[2077] Ibid.

Tanzania is a constitutional multi-party democracy. The URT Constitution 1977 is the supreme law. Any law or conduct that contravenes the Constitution becomes invalid.[2078] There is a similar provision in the Constitution of Zanzibar 1984.[2079] The executive powers in the United Republic are vested in the President of the United Republic while for Zanzibar, the President of the Revolutionary Government of Zanzibar.[2080] Legislative powers are vested in the Parliament of the United Republic of Tanzania and Zanzibar House of Representatives.[2081] In both cases the legislature consists of the President and National Assembly. The latter is largely composed of elected representative of the people. It is imperative to note that currently the ruling party *Chama Cha Mapinduzi* (CCM) has majority seats in the Parliament of the United Republic of Tanzania and the Zanzibar House of Representative.

The legal system in the United Republic of Tanzania and Zanzibar follows the English common law. However, judiciary is not generally a union matter. Hence the United Republic of Tanzania has its own judiciary while Zanzibar has also its own. Yet, the Court of Appeal of Tanzania (the Supreme Court) is a union matter. It means that appeal originating from the High Court of Tanzania (serving mainland Tanzania) and from the High Court of Zanzibar (excluding Islamic matters) may be filed in the Court of Appeal of Tanzania (CAT). Below the High Courts of Tanzania and Zanzibar there are subordinate courts with limited jurisdictions.

The Tanzanian socialism based on *Ujamaa* ideology is the major determinant of the Tanzanian socio-economic and political context. *Ujamaa* as an ideology started formally with the Arusha Declaration of 1967. Summarising the basic tenets of this ideology, Karim F. Hirji posits:-

> 'While Mwalimu Nyerere[2082] had talked about socialism from the early days of *Uhuru*, the Arusha Declaration of 1967 marked the first serious step in that direction. The Declaration envisioned a society based on equality, service for the common good and justice for all. It advocated public ownership of the major means of production and other pillars of the economy; it sought to extricate the masses from poverty, ignorance and disease by establishing *Ujamaa* villages; and it limited the private income-generating activities of political and governmental leaders to prevent the emergence of a privileged

[2078] URT Constitution 1977, Arts 30(5) and 64(5).
[2079] Katiba ya Zanzibar ya 1984, Ibara ya 4.
[2080] URT Constitution 1977, Art 4(1) and Katiba ya Zanzibar ya 1984, Ibara ya 26.
[2081] Ibid, Art 64 and Ibara ya 78 respectively.
[2082] Julius Kambarage Nyerere, commonly known as Mwalimu (i.e. Teacher) was the first President of Tanzania.

> stratum cut off from and ruling over the common man. It also stated that these goals would be achieved primarily with internal, national efforts, and not through reliance on foreign funds or supports.'[2083]

It is imperative to note that, in order to impart, instil and consolidate the *Ujamaa* ideology in the minds and daily lives of Tanzanians, political leaders coined various terminologies to be used against practices that were anti-*Ujamaa* values. Brennan points that the Swahili words: '*Unyonyaji*', '*Kupe*', '*Kabaila*', '*Bwanyenye*', and '*Bepari*' which in different contexts signified someone who lives by exploiting others, were commonplace in order to shun individuals who were not upholding *Ujamaa*.[2084] It was therefore not by accident that *Ujamaa* was the main justification for the nationalisation of private properties: commercial banks, insurance firms, sisal industry, textile industries, wholesale trade, etc.[2085] Through nationalisation, the state became the main producer of goods and services. This marked the beginning of the command economy and mushrooming of parastatals.

Ujamaa worked for sometime. However, it soon failed due to various reasons. One of them was lack of proper implementation of the ideology. For example, in the field of agriculture, *Ujamaa* was used to force citizens to live in *Ujamaa* villages and farm together. The '*Operation Vijiji*' or '*Villagisation*' as the programme was referred to, received little public support. Together with other reasons, lack of public support collapsed the '*Operation Vijiji*'.[2086] Yet, there were some other reasons beyond the implementation of *Ujamaa* policy. There is a large degree of consensus among scholars that the collapse of *Ujamaa* is largely the function of events that occurred between 1970s and 1980s.[2087] During this period, Tanzania experienced economic crises triggered off by such factors like the Oil Crisis of 1973, Kagera War 1978/1979 between Tanzania and Uganda, the collapse of the East African Community in 1977 and the persistent drought conditions.[2088] As alluded to, globally there was the collapse of U.S.S.R following the end of the

---

[2083] Hirji, K.F., 'Socialism Yesterday' in Hirji, K. F(ed)., CHECHE: Reminiscences of a Radical Magazine, Mkuki na Nyota, Dar es Salaam, 2010, pp.134-154, at p.135.
[2084] Brennan, J.R., 'Blood Enemies: Exploitation under Urban Citizenship in the Nationalist Political Thought of Tanzania, 1958-75', Journal of African History, 2006, Vol.47, No.3, pp.389-413.
[2085] See e.g., Katunzi, J., 'Managing Change in Tanzania Public Enterprises: Swallowing Bitter Pills', The IFM Journal of Finance and Management, 1998, Vol.6, No.2, pp.14-23, at p.15.
[2086] For detailed discussion about Villagisation in Tanzania and its collapse see e.g., Lofchie, M., 'Agrarian Crisis and Economic Liberalisation in Tanzania', The Journal of Modern African Studies, 1978, Vol.16, No.3, pp.451-475; Briggs, J., 'Villagisation and the 1974-6 Economic Crisis in Tanzania', The Journal of Modern African Studies, 1979, Vol.17, No.4, pp.695-702; Ergas, Z., 'Why Did the Ujamaa Village Policy Fail?-Towards a Global Analysis', The Journal of Modern African Studies, 1980, Vol.18, No.3, pp.387-410.
[2087] See e.g., Makulilo, A.B., 'State-Party and Democracy: Tanzania and Zambia in Comparative Perspective', PhD Thesis, University of Leipzig , 2010, p.25.
[2088] Ibid.

Cold War. The U.S.S.R was the main supporter of socialist system of which Tanzania was one of the beneficiaries. To address the economic crises of 1970s-1980s, Tanzania approached the IMF/WB and the international donor community.[2089] As a condition for loan and other financial assistance, the IMF/WB and the international donor community imposed the SAPs with key demands for political and economic liberalisation. Specifically, SAPs demanded currency devaluation, removal of government involvement and allow the market mechanism to operate through the impersonal forces of supply and demand, elimination of subsidies, liberalisation of trade and politics.[2090] Generally, the implementation of SAPs resulted into significant shifts of socialist policies and ideology in Tanzania: from *Ujamaa* to capitalism. *Ujamaa* was tactfully abandoned in the Zanzibar Declaration of 1991.[2091] This policy shift was immediately followed by privatisation of the economy as well as political liberalisation.[2092] Some commentators have unconvincingly argued that there was a favourable public mood that provided opportunity for privatisation, though there was no consensus on how to privatise.[2093] However the opposing view has been repeated by influential scholars such as Professor Issa Shivji:-

> 'This so called new form of foreign investments that we are rushing for will not do us any good. They are coming just to take away our resources and leave us with nothing. A good example is in the mineral sector. We are only left with 3% of what has been taken out of our land and they go with 97%. If this is not rape, what is it? They have had negative impact on the overall aspect of business and human rights, cooperate governance and good governance in general.'[2094]

Despite the shift in policy through SAPs from *Ujamaa* to neo-liberal ideology; and the actual privatisation of parastatals, the URT Constitution 1977 maintains that Tanzania is a 'socialist state'.[2095] The same constitution provides further that its object is to build a nation of equal and free individuals through the pursuit of 'the policy of Socialism and Self-Reliance which emphasises the application of socialist principles'.[2096] Some commentators have argued that the

---

[2089] Ibid.
[2090] Riddell, B., 'Things Fall Apart Again: Structural Adjustment Programmes in Sub-Saharan Africa', The Journal of Modern African Studies, 1992, Vol.30, No.1, pp.53-68, at pp.57-59.
[2091] Makulilo, A.B., 'CCM at 34 and the Deepening Crisis', The Citizen, 4th February 2011.
[2092] See generally, Michael, A., 'The Decision and Implementation of Privatization in Tanzania', M.A Thesis, Institute of Social Studies, The Netherlands, 2002.
[2093] Ibid, p.28.
[2094] Shivji, I., 'Current Investors plunder Our Resources', The African, 3rd December 2009.
[2095] URT Constitution 1977, Art 3(1).
[2096] Ibid, Art 8.

continued retention of *Ujamaa* in the URT Constitution 1977 provides a significant tool for voters' mobilisation by the CCM ruling Party.[2097] This is because, majority of Tanzanians are still favourable to *Ujamaa* as they were able to access free social services.[2098]

As pointed out, the socio-economic and political context in Tanzania is still based on *Ujamaa* despite the existing neo-liberal policies. For example, although in 1992 Tanzania adopted multi-party political system, in what can be termed as political liberalisation, the actual practice is still centred on the single party regime. In his book, *'Tanzania: A De facto One Party State?'* Makulilo has systematically analysed the legal regime and entire political environment in Tanzania only to find that they are all operating in favour of the ruling party.[2099] It has similarly been observed that many African countries (including Tanzania) embraced multipartism without the will to liberalise the political space in terms of the institutional arrangement, legal framework and behavioural change.[2100] Elections are only wanted if they yield the predetermined results in favour of governing regimes.[2101] Yet, there are some areas which have significant changes. For example, the Tanzania economy has opened up. Most of the public enterprises have been privatised. The former President Benjamin Mkapa, under whose presidency the privatisation was largely carried out, pointed out recently that a total of 386 parastatals were privatised.[2102] Out of them 180 were privatised to local investors and only 23 to foreign investors.[2103] He also pointed out that the government sold shares in the remaining corporations and industries.[2104] Yet, Mkapa has strongly been criticised by Professor Issa Shivji that it was wrong for the government to privatise important sectors such as banks and insurance.[2105] It is important to note that, the general view is that privatisation has not improved the performance of corporations and industries in Tanzania.

Technologically, Tanzania has come far. As pointed out, after independence, particularly in 1974, Tanzania banned the importation of computers and related equipments in the country.[2106] This

---

[2097] Makulilo, p.32, note 2087,supra.
[2098] Chaligha *et al*, p.20, note 2074, supra.
[2099] Makulilo, note 1150.
[2100] Bakari, M and Makulilo, A., 'Beyond Polarity in Zanzibar? The "Silent" Referendum and the Government of National Unity', Journal of Contemporary African Studies, 2012, Vol.30, No.2, pp.195-218, at p.211.
[2101] Ibid.
[2102] 'Mkapa defends privatisation, blames bad management', The Citizen, 14th April 2012, http://www.thecitizen.co.tz/news/-/21464-mkapa-defends-privatisation-blames-bad-management, last visited 26/04/2012.
[2103] Ibid.
[2104]Ibid.
[2105] Ibid.
[2106] Mgaya, K., 'Development of Information Technology in Tanzania' in Drew, E.P and Foster, F.G (eds)., Information and Technology in Selected Countries: Reports from Ireland, Ethiopia, Nigeria and Tanzania, University of United Nations, Tokyo, 1994,

was done through the Government Gazette.[2107] However, in the late 1980s the ban was lifted and by 1990s, there was proliferation of computers in the country and their increasing usage in the public and private sectors.[2108] The importation of the mobile phone technology in 1990s as well as the Internet particularly around 2000s, has seen the penetration of ICTs in Tanzania. A survey conducted by the Tanzania Regulatory Communications Authority (TCRA) reveals that by June 2010, Tanzania had an estimated number of 4.8 million internet users.[2109] Out of this number, only 5% used internet services from cyber cafes, 55% used internet from organisations or institutions, and 40% from households.[2110] In terms of penetration, the survey reveals that only 11% of Tanzanians were accessing and using internet services.[2111] On the other hand, by March 2010, there were more than 17 mobile phone users in Tanzania.[2112]

Socially, Tanzanians are individualist and collectivists as well. Yet, the latter is dominant as Professor Geert Hofstede posits:-

> 'Tanzania, with a score of 25(measured in value range from 0 to 100) is considered a collectivist society. This is manifest in a close long-term commitment to the member "group", be that a family, extended family, or extended relationships.'[2113]

It is imperative to note that *Ujamaa* has largely contributed to collectivist culture in Tanzania. However, Westernisation aided with ICTs is fast changing individuals' relationships both in the urban and rural Tanzania.[2114] The impact of westernisation has also been captured by the music industry. In his famous song '*Mnyonge Hana Haki*' (i.e. The Poor Have No Rights), Remmy Ongala opened the song with the phrase 'Mother-where are you?' suggesting that he is separated

---

http://archive.unu.edu/unupress/unupbooks/uu19ie/uu19ie0i.htm#4:%20development%20of%20information%20technology%20in%20tanzania, last visited 26/04/2012.

[2107] Ibid.

[2108] Makulilo, A.B., 'The Admissibility of Computer Printouts in Tanzania: Should it be any Different Than Traditional Paper Document?', LL.M Thesis, University of Oslo(Norway), 2006, p.2.

[2109] Tanzania Communications Regulatory Authority (TCRA)., 'Report on Internet and Data Services in Tanzania: A Supply-Side Survey', September 2010, p.2, http://www.tcra.go.tz/publications/InternetDataSurveyScd.pdf, last visited 26/04/2012.

[2110] Ibid.

[2111] Ibid.

[2112] 'Mobile Phone Users now top 17 million', The Citizen, 19th March 2010.

[2113] Hofstede, G., 'Tanzania', http://geert-hofstede.com/tanzania.html, last visited 26/04/2012.

[2114] See generally, FitzGerald, J.R.S., 'The Last of the Maasai in Northern Tanzania?-Redefining Cultural Identity', M.A Thesis, Oxford Brookes University, 2008.

from his family.[2115] Moreover, in the same song Ongala makes more explicit about the pressures of liberalisation, competition and inequality in urban areas where he sings that 'in Dar es Salaam everyone is on his/her own'.[2116]

The loss of cultural ties both as a result of Western Christian and urban life-style in Tanzania had been considered by the High Court of Tanzania in oft-quoted case of *Re Innocent Mbilinyi*[2117] well before liberalisation. This case involved the estate of the late Innocent Mbilinyi in which his relatives wished his estate to be administered under customary law. On the other hand the deceased's widow wished her husband's estate to be administered through the Indian Succession Act 1865 which is applicable to Christians in Tanzania. Both Innocent Mbilinyi and his wife were Christians, and they contracted a Christian marriage. However, they belonged to different tribes: Ngoni and Chagga, respectively. After marriage they lived in urban areas including Dar es Salaam (the Capital City of Tanzania by then). In its ruling, the High Court held that the deceased had abandoned the customary way of life in favour of a Christian one. Together with the fact that Innocent Mbilinyi lived in Dar es Salaam after marriage and worked there, the court ruled further that he had alienated from his family and that his children had no connection whatever with them. The High Court of Tanzania directed that the Indian Succession Act was applicable in the administration of the deceased estate.

In terms of health, Tanzania, just like many other sub-Sahara African countries, is affected by HIV/Aids. By 2009, it is estimated that Tanzania, with a 5.6% adult prevalence HIV/Aids rate, ranked twelfth in the world.[2118] The statistics indicate also that in 2009, there were 1.4 million people living with HIV/Aids, making the country ranks the sixth in the world.[2119] By the same year, an estimated number of 86,000 people lost their lives through HIV/Aids, the record that ranked Tanzania the fourth in the world.[2120] A monthly published magazine, *'Tanzania AIDS Week in Review'*[2121] has estimated that by March 2012, the national prevalence of HIV/Aids in Tanzania mainland stood at 5.7% down from 7 in 2004, suggesting a declining rate though at a

[2115] Hilhosrst, S., 'Remmy Ongala: Capitalist Transition and Popular Music in Tanzania 1979-2002', Journal of African Cultural Studies, 2009, Vol.21, No.2, pp.105-126, at p.120.
[2116] Ibid.
[2117] [1969]H.C.D 283.
[2118] CIA World Factbook 2012.
[2119] Ibid.
[2120] Ibid.
[2121] Tanzania AIDS Week in Review, Issue No.161, February 26-March 3, 2012, http://www.ajaat.or.tz, last visited 27/04/2012.

slow pace. Yet, on its website, the magazine provides extra information that the HIV/Aids population in Tanzania now stands at 1.8 million.[2122]

7.3 Social Attitudes to Privacy

Privacy is less prominent a public issue in Tanzania. However there are isolated cases and trends for claim for privacy which can give a wider picture of Tanzanians' attitudes towards privacy. Debates on the registration of SIM cards comprise one of these isolated cases and trends.[2123]

In January 2009 the Tanzania Communications Regulatory Authority (TCRA) announced that all existing and future subscribers of pre-paid SIM cards must be registered.[2124] This public notice required mobile service providers to maintain databases of information of their subscribers. Included in such databases are information on the phone number, name, date of birth, gender, address, alternative phone numbers(if available), the number on ID card, passport, driving licence, student card, voter registration card, or a letter from a local government official. The deadline for registration was initially set for six months i.e. from 1 July 2009 to 31 December 2009. However, this limitation period was extended for another period of six months to 30 June 2010[2125] and subsequently for half a month to 15 July 2010.[2126]

TCRA advanced four reasons in support for registration of pre-paid SIM cards: to protect consumers from misuse of communication services, to enable consumers to be identified as they use value added services, such as mobile banking, mobile money transfer, electronic payments for services such as water, electricity, pay-TV etc, to enhance national security and to enable network operators to promote "know your customer."[2127] In the beginning, the TCRA's directive to service providers provided the basis for collection of personal information from their subscribers.[2128] However this directive was not backed by any statutory law. Legislation on

---

[2122] AJAAT Website, http://ajaat.or.tz/home/index.php last visited 27/04/2012.
[2123] Discussion in this part is partly adopted from Makulilo, notes 224 and 225, supra.
[2124] TCRA., 'Public Notice: SIM Card Registration', http://www.tcra.go.tz/headlines/simcardRegEng.pdf, last visited 27/04/2012; See also, DAILY NEWS, 29th January, 2009, p.3.
[2125] TCRA., 'Press Release: SIM Card Registration',http://www.tcra.go.tz/headlines/SimRegPublicNoticeEn.pdf, last visited 27/04/2012.
[2126] The Guardian, 1st July, 2010, pp.1-2; See also, THE CITIZEN, 1st July, 2010, p.2.
[2127] These reasons were explained in the subsequent notices for extension of SIM registration (see footnotes 2122 and 2123 supra). However the initial public notice (see footnote 2124 supra) indicated only security as the reason for SIM card registration.
[2128] TCRA's directive being administrative in nature would not satisfy the requirements of Article 16(2) of the Tanzanian Constitution which requires that any derogation to the constitutional right to privacy enshrined in Article 16(1) of the Constitution must lay down legal procedure for that derogation. Moreover it must pass the proportionality test.

mandatory registration of SIM cards only came into force towards the end of the registration exercise. Yet, the need for registration of SIM cards first occupied the Tanzanian Parliamentary debates on 18 August 2008 well before the registration of SIM cards.[2129] Interestingly, protection of subscribers' right to privacy was a less priority concern for the legislators. It is imperative to note that during this session only one legislator raised concern over the right to privacy. However, since there was no Bill for SIM card registration tabled before the Parliament, no discussion took place over concern for privacy. It was until 27 January 2010 when the Government introduced the Electronic and Postal Communication Bill 2009 to the Parliament for its first reading that discussion took place. This Bill contained provisions for regulation of SIM cards. It was passed into law two days later, i.e. on 29 January 2010. Interestingly, no legislator raised concern over individual's right to privacy during parliamentary debates, not even the only legislator who warned breach of right to privacy on 18 August 2008 over a law on registration of SIM cards.

However, outside Parliament, some people raised serious objections to the registration of SIM cards on account of privacy concerns. Notable instances of such objections appeared on 28 January 2009 in the discussions of a thread, 'SIMCARD Registration in Tanzania now a MUST' on JamiiForums.[2130] Discussants were concerned with registration of SIM cards without having in place national ID cards, casting doubt on the information quality and reliability. The other aspect widely raised in the discussion was the lack of proper legal safeguards against interception of private communication by the government and service providers themselves. Similar concerns for privacy appeared in the headlines of newspapers. For example, the Arusha Times bore the headline, 'SIM-card registration now viewed as spying move'.[2131] It was generally feared by many people that SIM card registration that was going on since 2009 was aimed at spying their political interests and loyalties during the 2010 general elections.[2132] A more critical article, *'Kusajili simu za mkononi ni uhalifu'*[2133] translating in English, 'Registering mobile phone is a crime' argued that 'the government and the mobile phone service providers have conspired with the mobile phone

[2129] See, BUNGE LA TANZANIA, MAJADILIANO YA BUNGE, MKUTANO WA KUMI NA MBILI, Kikao cha Arobaini na Saba – Tarehe 18 Agosti, 2008.
[2130]JamiiForums, 'SIM Card Registration in Tanzania Now a Must', discussions held on 28th January, 2009http://www.jamiiforums.com/jukwaa-la-siasa/23569-simcard-registration-in-tanzania-now-a-must.html, last visited 27/04/2012.
[2131]The ARUSHA TIMES., 'Tanzania: SIM-Card Registration Now Viewed As Spying Move', 7-13 November 2009, http://www.arushatimes.co.tz/2009/44/front_page_3.htm, last visited 27/04/2012.
[2132] Ibid.
[2133] Tanzania Daima Jumapili, Julai 26, 2009, uk 5.

operators in carrying out SIM card registration. They have agreed to intercept citizens' private communications. Perhaps they have been doing so for long a time.'[2134]

There are specific privacy incidents which are related to SIM cards. Most of them have raised serious concerns for individuals' privacy. For example, in September 2010 there was a widely circulation of a hoax text message in Tanzania warning people that they would die if they received calls whose numbers were in red. The message raised fear and panic to most Tanzanians. Due to this, some people challenged the registration of SIM cards which aimed at enhancing security from misuse of mobile phones.[2135] At the same time, there were defamatory and hateful text messages circulated to millions of Tanzanians during the political campaigns for the last 31 October 2010 General Elections.[2136] These messages defamed and unreasonably attacked the presidential candidates for the two opposition parties: *Chama cha Demokrasia na Maendeleo* (CHADEMA) and the Civic United Front (CUF). However what puzzled many people was how the author of the massage managed to access the database of various mobile phone operators in order to reach millions of people countrywide directly.[2137] The concern for privacy was exacerbated by the fact that under normal circumstances, no mobile handset can store that volume of contacts, but the mysterious author managed to jam over 5 million users within 48 hours, causing panic and outrage among opposition supporters.[2138]

Still in relation to the general elections carried in October 2010, the Director of the Prevention and Combating of Corruption Bureau (PCCB) confirmed to the general public that, his entity had the technology to monitor and identify people dishing out bribes through mobile cash transfer (i.e. Vodacom's M-Pesa; Zain's Zap and Tigo Pesa of Tigo).[2139] The context in which the PCCB issued its statement was the elections which are usually tainted with bribes. In contrast, the Vodacom Tanzania's head of public relations and corporate social responsibility, Ms. Mwamvita Makamba refuted PCCB's statement by holding that the mobile company had not received any complaints from any agency, including PCCB, about the abuse of its mobile money

---

2134 Ibid.
2135 See e.g., The Guardian, 6th September, 2010, pp.1-2; The Guardian, 7th September, 2010, pp.1-2; The Guardian, 12th September, 2010, pp.1-3,18; THE CITICEN, 6th September, 2010, p.8; DAILY NEWS, 9th September, 2010, p.1; Dar Leo, 8th September, 2010,p.1 & 4, UWAZI, 14-20, Septemba, 2010, pp. 1 & 3; and SANI, 11-14, Septemba, 2010, pp.1-2.
2136 The Guardian on Sunday., 'Revealed: Kingpin behind "hateful" text messages', 17th October, 2010, http://www.ippmedia.com/frontend/index.php?l=22119 last visited 27/04/2012.
2137 Ibid.
2138 Ibid.
2139 THE CITIZEN., 'PCCB has eye on mobile cash transfer', 6th September 2010, p.2.

transfer.[2140] Surely, these opposing statements had left Tanzanians who use mobile cash transfer in a state of dilemma.

Newspapers have also raised privacy concerns to Tanzanians. Some of them have published photographs depicting the likeness of individuals without authorisation. For example, in 2005, Mwananchi Communications Ltd, published in its two newspapers *Mwananchi* and *the Citizen* a commercial advertisement using the likeness of Ms. Sia Dominic Nyange who participated in the Miss Tanzania Beauty Pageantry 2004. The advertisement was circulated countrywide for about three months. In reacting to the publication of her likeness without her consent, Ms. Nyange instituted a civil suit against the company alleging violation of her right to privacy.[2141] It is interesting to note that, in this case the company opted to settle the matter out of court by compensating Ms. Nyange, suggesting an admission of the violation her right to privacy.

The other instance for claim of privacy against a newspaper is provided by *Mkami Kasege & Ismail Msengi v Risasi.*[2142] In this case, the complainant instituted a claim against a newspaper, *Risasi* (owned by the Global Publishers Ltd) in the Media Council of Tanzania. Her complaint was about publication of false and malicious articles which had seriously damaged her reputation and invaded her privacy. One of the articles published in the *Risasi* tabloid appeared with a headline, *'Za mwizi fote'* translating in English as *'A thief's 40 days are over'*. This article purported that Ms. Kasege had been caught two-timing with lovers while she was a married woman. In a follow-up story carried by *Risasi* under the headline *'Ticha aliyefumaniwa anywa sumu'* translating in English as *'two-timing teacher attempts suicide'*, it was alleged that Ms. Kasege attempted to kill herself because of the conflict between her lovers. Moreover she had ended up in a police case. Ms. Kasege was particularly concerned with private photographs which were published by the newspaper that showed her in a semi-nude state. This case was heard *ex-parte* since the editor of *Risasi* newspaper refused to attend the hearing. It was revealed in this case that the allegations raised in *Risasi* were not true. Based on that, the Media Council held that guidelines on privacy of individuals were clearly spelt out in the Code of Ethics for Media Professionals. It went on to hold that even in the case of public figures that usually have little protection of their privacy from the media, it is only acceptable to intrude in their privacy when it is absolutely necessary in the public interest. The Council observed that it was gravely concerned by the unacceptable trend of some tabloids

[2140] Ibid.
[2141] Sia Dominic Nyange v Mwananchi Communications Ltd, Civil Case No. 155 of 2005, the Resident Magistrate's Court of Dar es Salaam, at Kisutu (Unreported).
[2142] Conciliation Case No. 1 of 2005, 1997-2007, MCT 111.

that continuously invaded the privacy of individual citizens and exposed them to humiliation and unnecessary anguish. In the end, the Council ordered the Editor of *Risasi* newspaper to retract the story, apologise to the complainants and pay the costs incurred by the complainants. It is important to note that, the newspaper did not comply with the decision of the Council. Part and parcel of the non-compliance to this decision is the fact that the Media Council of Tanzania is a voluntary, self-regulatory body. It does not have powers to issue binding legal decisions rather it reconciles parties.

Certain newspapers have intercepted private communication and published contents of their messages. For example, on 11-14 July 2009, *Sani* published an SMS implicating one of the Tanzanian female celebrities to have an affair with a married man.[2143] These kinds of messages are common in some Tanzanian newspapers. Partly due to this, some legislators have raised serious concerns with regard to violation of privacy by newspapers. To be sure, on 14 July 2011, Ms. Martha Mosses Mlata, a legislator, said:-

> 'Honourable chairperson, some newspapers have dared to interfere with individuals' mobile phone communications including politicians. However, TCRA (Tanzania Communications Regulatory Authority) has not taken any action against perpetrators including mobile phone operators. We have seen in other countries actions have been taken to suspend such newspapers. For example, few days ago, in the United Kingdom, the News of the World has been abolished. Why does TCRA fail to take action? We request the government to empower TCRA to take actions, otherwise this state of affair amounts to interfering with an individual's freedom. It is also humiliation and violation of human rights."[2144]

Somewhat related to above are concerns for privacy from unsolicited text messages (SMSs) sent by mobile phone operators. Individuals' protests to these massages can well be demonstrated by two appealing newspaper headlines, *Airtel bothering me with unwanted text messages* and *Yes, unwanted*

[2143] Sani., 'Mume wa Mtu amliza Wema', 11-14 Julai 2009.

[2144] Translated in English from original Kiswahili language: 'Mheshimiwa Mwenyekiti, baadhi ya magazeti yamediriki kuingilia mawasiliano ya simu ya watu fulani wakiwemo wanasiasa na kuchapisha magazeti, lakini TCRA imekuwa haichukui hatua kwa wahusika ikiwemo kampuni za simu. Tumeona nchi zingine zikichukua hatua pamoja na kuyafungia. Kwa mfano, juzi yalitokea Uingereza kufungiwa kwa gazeti la News the World. Je, ni kwa nini TCRA hawachukui hatua? Tunaomba sana Serikali iiongezee nguvu na ipewe uwezo wa kuchukua hatua, vinginevyo hali hiyo ni ya kuingilia uhuru wa mtu na pia ni udhalilishwaji na ni kukiuka haki za binadamu', see Parliament of Tanzania, Parliamentary Questions and Answers, Session No. 4, Seating No. 4, 14 July 2011.

Airtel SMS a pain in the neck published in the Citizen of 26 July 2011 and 11 August 2011 respectively.[2145] As alluded to, the concerns for privacy here stemmed from unsolicited SMS by the Airtel, a mobile phone operator in Tanzania. During this period, Airtel sent unsolicited SMSs urging individuals to take part in some competition and win million of money. On average, Airtel's customers received up to 20 of unwanted SMSs daily. These messages clogged the customers' inboxes, forcing them to delete the messages every now and then. Surprisingly,when customers tried to call the Airtel's customer care number with the intention of telling the company to stop sending them the SMSs, the number was permanently unavailable. The worse part of it was that, the customers were not given option to decide whether or not they wanted to take part in the 'competition'. Customers also complained against the Tanzania Communications Regulatory Authority for assuming the role of a bemused spectator.

Perhaps one of the most incidents of privacy concerns that did not go unnoticed by many Tanzanians involved the eavesdropping devices placed in the hotel rooms of Dr. Willbroad Slaa and Dr. Ali Taarab Ali in February 2009. Both Dr. Slaa and Dr. Ali were members of Parliament from the opposition camp, attending parliamentary sessions. Later in 2010, Dr. Slaa became a presidential candidate for CHADEMA, one of the strongest opposition parties in Tanzania. Some of the newspaper headlines which captured the incident read, 'Big Brother is watching you!';[2146] 'MPs hotels bugging claim under police probe';[2147] and 'MP Slaa blasts police over spy bug incident.'[2148] No one has been arrested to date in connection with the incident.

The use of Internet has also raised concerns for privacy. One of the areas which has generated such concerns are interceptions of email communications. For example, in June 2009, there was widely circulated news in the media of Tanzanians whose email accounts were intercepted by fraudsters. Most of these emails claimed their senders to have been stranded in far-off countries like Nigeria, etc. They also informed their recipients that they had lost or had been robbed of their wallets, passports and air tickets, and asked for some money to somehow get home.[2149] It is imperative to note that, apart from fraud purposes, interception of email has been invoked to

[2145] THE CITIZEN, 26th July 2011, http://www.thecitizen.co.tz/editorial-analysis/20-analysis-opinions/13167-airtel-bothering-me-with-unwanted-text-messages.html last visited 29/04/2012; THE CITIZEN 11th August 2011, http://www.thecitizen.co.tz/editorial-analysis/46-letters-to-the-editor/13658-yes-unwanted-airtel-sms-a-pain-in-the-neck.html last visited 29/04/2012.
[2146] Daily News, 12th February 2009.
[2147] Daily News, 6th February 2009.
[2148] JAMIIFORUMS, http://www.jamiiforums.com/habari-na-hoja-mchanganyiko/29145-dr-slaa-polisi-tanzania-ni-kitengo-cha-ccm.html last visited 29/04/2012.
[2149] 'International con artists tap into local email accounts', THISDAY, 24th June 2009; see also, 'Utapeli wa mtandao wawaliza wengi nchini', KULIKONI, 24 Juni 2009.

target radical politicians. One of the instances for such interception was reported in *MwanaHalisi* tabloid with a headline, *'Siri za Zitto nje'* translating in English as 'Secrecy of Zitto out'.[2150]

The other area resulting in privacy concern over the Internet relates to the most controversial blog called *'Ze Utamu'*. This blog is no longer operating. *Ze Utamu* used to publish pornographic photographs of individuals. In one occasion, the blog published the photograph of the current president of the United Republic of Tanzania, Mr. Jakaya Mrisho Kikwete.[2151] It was at this point that the government intervened to arrest its owner who was a Tanzanian-British citizen. The settlement of the matter culminated into shutting down of the blog.

Health privacy has also generated a lot of concerns. The most sensitive aspect of such concerns is about HIV/Aids. This is probably because of the stigma surrounding it. One of the recent incidents which has raised the attention of not only Tanzanians but also the world, is the requirement for HIV positive pupils to wear ribbons in some of the Tanzanian schools. In reporting this concern, *the Independent* bore the heading, 'Tanzanian pupils with HIV "forced to wear ribbons."'[2152] According to the school's authority, the identification of these pupils was meant to exclude them from strenuous activity. On its part, the Amnesty International has required Tanzania to end HIV stigma in schools through 'red ribbon'.[2153] It is interesting to note that in refuting the truth of the claim, the Regional Commissioner of the Coastal Region where the 'red ribbon' stigma was reported, defended that those pupils with 'red ribbon' were suffering from other diseases, particularly the heart disease.[2154]

HIV/Aids has also been a concern in the employment sector. Previous studies conducted in this filed have revealed that it is an established practice in Tanzania for employers in the public and private sectors to require pre-employment medical test for new employees.[2155] This practice has generated privacy concerns in the employment sector because such medical tests involve secrete

---

2150 'Siri za Zitto nje' MwanaHalisi, 9-15, Desemba 2009.
2151 'Mzee wa Ze Utamu anaswa', MWANANCHI, 20 Juni 2009; See also, 'Ze Utamu bares local Police who walk away with a vendor's table caught selling at a prohibited area', DAILY NEWS, 27th June 2009.
2152 The INDEPENDENT, 16th March 2012, http://www.independent.co.uk/news/world/africa/tanzanian-pupils-with-hiv-forced-to-wear-ribbons-7574470.html last visited 29/04/2012; See also, BBC News., 'Tanzania anger over red ribbon labels for HIV pupils', 15th March 2012, http://www.bbc.co.uk/news/world-africa-17380941 last visited 29/04/2012.
2153 Amnesty International., 'Tanzania must end HIV "red ribbon" stigma in schools', 16th March 2012, http://www.amnesty.org/en/news/tanzania-must-end-hiv-red-ribbon-stigma-schools-2012-03-16, last visited 29/04/2012.
2154 In2EastAfrica., 'RC refutes reports on Tanzania pupils' HIV/Aids stigma', http://in2eastafrica.net/rc-refutes-reports-on-tanzania-pupils-hivaids-stigma/ last visited 29/04/2012.
2155 Makulilo, note 224, supra.

HIV testing. This is partly due to the fact that with the rapid decrease in the workforce and revenues and increasing sick leave costs as a result of HIV/Aids, many employers in Tanzania are reluctant to employ persons who are HIV positive.

Similarly, health privacy has raised concern in other aspects other than HIV/Aids. Probably the most recent illustration is the 'Mwakyembe saga' which has drawn the attention of the media and public. The latter involved the revelation of health information of one prominent politician, Dr. Harrison Mwakyembe, the Deputy Minister for Works. Following the recent ill health of Dr. Mwakyembe, there were claims by people around him and at times Dr.Mwakyembe himself that he was poisoned. He received treatment in India. Later the Director of Criminal Investigation (DCI), Robert Manumba, issued a report that the ill health of the Deputy Minister for Works was not caused by poison.[2156] The DCI's report confirmed to have contacted the Ministry of Health and Social Welfare about Mwakyembe's claims. Part of the DCI's report indicated that the Ministry for Health and Social Welfare had contacted the doctors who attended Dr. Mwakyembe in India to know about the disease he was suffering from. Dr. Mwakyembe alleged breach of the principle of doctor-patient confidentiality. As a result, the Ministry for Health and Social Welfare issued a statement that it had never contacted anybody in India about Dr. Mwakyembe's health nor did it inform the DCI about the health information about the Deputy Minister for Works.[2157]

It is interesting to note that, sometimes before the Mwakyembe's saga, the Tanzanian President's health was publicly revealed in detail in a news conference by his personal physician. Yet, there was no claim by the President that his health privacy had been divulged. Part of the reason was that, the disclosure was authorised by the President. Moreover, before he revealed such health information the President's physician clearly pointed out that he had been obliged to breach normal doctor-patient confidentiality at the request of the President himself.[2158]

Other areas which have touched upon individuals' privacy in Tanzania include the current project on National Identity Card; smart driving licences; the planned project for CCTV in Dar

---

[2156] THE CITIZEN., 'Mwakyembe was not poisoned, say police', 18th February 2012, http://thecitizen.co.tz/news/4-national-news/19863-mwakyembe-was-not-poisoned-say-police.html, last visited 30/04/2012.
[2157] THE CITIZEN., 'Mwakyembe saga raises concern over team spirit', 20th February 2012, http://thecitizen.co.tz/news/4-national-news/19947-mwakyembe-saga-raises-concern-over-team-spirit.html, last visited 30/04/2012.
[2158] THISDAY., 'Revealed: JK's health in detail', 9th October 2009.

es Salaam; voter registration database; and biometric passports. Yet, there have been no strong privacy debates or concerns raised in relation to these privacy invasive activities.

One recurring reason affecting negatively privacy concerns in Tanzania is lack of awareness. It has been argued by some Tanzanian commentators that lack of awareness is a paramount factor resulting in little privacy consciousness by individuals. To be sure Ubena posits:-

> 'I know not so many Tanzanians are aware of how communication service providers are using customers' personal information. They are using such information for marketing purposes. They also use such information to evaluate their businesses. Hence monitoring and surveillance in Tanzania is (sic) rampant particularly online surveillance. As that is not enough, one will be surprised as the surveillance is not done by website owners or communication service providers only but even employers are reading employees' emails, this for sure is surveillance. Thus Tanzanians' privacy is not secured.'[2159]

The above observations are also shared by Mjasiri who argues that consumers in Tanzania are docile and have no audacity to demand their rights.[2160] However, unlike Ubena, Mjasiri has gone far to assign reasons for this state of affair. He has pointed lack of consumer education, the remnants of socialist economy which was command-based, and bureaucracy.[2161] Somewhat similar to Mjasiri's view, Bakari argues:-

> 'Another problem is that of culture. Based on my own experience and being part of the society, I can describe Tanzanians as characterised by generosity that affects not only material exchange, but also information exchange. Because of this generosity, you may ask to know about one thing and end up with a lot more information.'[2162]

While the above observations are overstated, they may partly reflect some truth particularly in rural areas. Be as it may, *Ujamaa* has its effects still prevailing in Tanzania. It is important to

---

[2159] Ubena, J., 'Tanzania lag on privacy law', Tanzania Legal News, posted on 8th June 2010, http://tanlex.wordpress.com/ last visited 30/04/2012.
[2160] Mjasiri, J., 'Consumers' rights "abused", lack of awareness to blame', Daily News, 13th March 2010.
[2161] Ibid.
[2162] Bakari, J.K., 'A Holistic Approach for Managing ICT Security in Non-Commercial Organisations: A Case Study in a Developing Country', Doctoral Dissertation, University of Stockholm, Sweden, 2007, p.9.

mention that lack of awareness does not only affect uneducated persons. Some Tanzanians who took part in the *Awareness Survey on freedom of Information and Data Protection Legislation and Open Government Data Initiatives*[2163] indicated that they were not aware of the existence or non-existence of a data protection law as well as a freedom of information law in Tanzania. Since some of them were affiliated to research or academic institution, it is clear that the field of data privacy is little known to educated persons as well. Yet, this state of affair is changing with time. For example, during an interview with the Head of Consumer Affairs at TCRA, it was confirmed that the regulator (i.e. TCRA) receives privacy complaints regularly.[2164] This is partly due to the efforts invested by TCRA to educate the public about their rights.[2165]

7.4 Legal and Regulatory Framework

As pointed out, Tanzania has no data privacy legislation. However three legal sources regulate privacy protection. The URT Constitution 1977 is the major source of the right to privacy. There are also various statutory provisions in different pieces of legislation which in an *ad hoc* fashion address privacy issues. Case law is the third source but quite insignificant at present. This part attempts to evaluate un-exhaustively these sources, particularly the statutory ones which are scattered in various pieces of legislation. However, particular emphasis is put on privacy in the health and communications sectors. This is partly because, the researcher had already undertaken researches in these sectors prior to the present thesis. Moreover, such researches culminated in the publication of two journal articles: 'You Must Take Medical Test: Do employers intrude into prospective employees' privacy?'[2166] and 'Registration of SIM cards in Tanzania: A critical evaluation of the Electronic and Postal Communications Act 2010.'[2167] These papers are relied in the present analyses.

7.4.1 The Constitution of the United Republic of Tanzania 1977

The URT Constitution generally guarantees the right to privacy in Article 16. The first limb of this provision states, '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

[2163] Taylor, note 1367, supra.
[2164] Interview held between the researcher of this thesis and Mr. Richard Kayumbo, (Head of Department Consumer Affairs, Tanzania Communications Regulatory Authority) on 7/09/2011 in Dar es Salaam, Tanzania.
[2165] Ibid.
[2166] Makulilo, note 224, supra.
[2167] Makulilo, note 225,supra.

residence and private communications.'[2168] However this right to privacy is not absolute. It is limited in Article 16 (2). This provision states, '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.'

Further restrictions to the constitutional right to privacy are generally provided in Article 30(2) of the Tanzanian Constitution. Article 30(2) states:-

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

The High Court of Tanzania (HCT) has quite often held that a law which seeks to limit or derogate from the basic right of individual on ground of public interest will be saved by Article

[2168] URT Constitution 1977, Art 16(1).

30(2) of the Constitution if it satisfies two requirements. Firstly, such law must be lawful in the sense that it is not arbitrary. This means that such law 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 must not be more than necessary to achieve the legitimate object. The second principle is sometimes called the principle of proportionality.[2169] In *Jackson Ole Nemeteni and 19 Others v the Attorney General*[2170] the HCT held that in the absence of a procedure prescribed by law, the administration of a provision of any law which seeks to limit the basic rights of an individual is susceptible to abuse, and cannot therefore be saved under Article 30(2) of the Constitution.[2171]

Up until recently there has been no specific case filed in the High Court of Tanzania alleging breach of constitutional right to privacy. This notwithstanding, the URT Constitution provides a normative basis for enactment of a data privacy legislation. Also important to note is that, the use of the expression 'every person...' in the beginning of Article 16(1) of the URT Constitution clearly suggests that the constitutional right to privacy in Tanzania can be enjoyed by citizens and non-citizens.

7.4.2 Electronic and Postal Communications Act 2010

The Electronic and Postal Communications Act 2010, commonly abbreviated as EPOCA, was passed by the Tanzanian Parliament on 29 January 2010 and assented by the President on 20 March 2010. The Act came into force on 7 May 2010.[2172] EPOCA repealed and replaced[2173] two pieces of legislation in the Tanzanian communication sector: the Broadcasting Services Act[2174] and Tanzania Communications Act.[2175] Also, the Act amended the Tanzania Communications Regulatory Authority Act[2176] and the Fair Competition Act.[2177] However it saved all regulations made under the repealed laws to the extent that they are not inconsistent with EPOCA and not

[2169] See for example, Kukutia Ole Pumbun and Another v Attorney General and Another [1993]TLR 159; Julius Ishengoma Francis Ndyanabo v Attorney General, Civil Appeal No. 64 of 2001, Court of appeal of Tanzania, Dar s Salaam(Unreported); Legal and Human Rights Centre and Others v Attorney General, Miscellaneous Civil Cause No. 77 of 2005, High Court of Tanzania, Dar es Salaam(Unreported); Christopher Mtikila v Attorney General, Miscellaneous Cause No.10 of 2005, High Court of Tanzania, Dar es Salaam(Unreported).
[2170] Misc. Civil Cause No. 117 of 2004, High Court of Tanzania, Dar es Salaam(Unreported)
[2171] The Court of Appeal of Tanzania had already considered this principle in the case of Director of Public Prosecutions v Daudi Pete [1993] TLR 22.
[2172] Government Gazette, No.19 of 7th May 2010.
[2173] EPOCA 2010, s.186.
[2174] Cap.306 R.E 2002.
[2175] Cap. 302 R.E 2002.
[2176] Cap.172 R.E 2002.
[2177] Cap. 285 R.E 2002.

expressly revoked.[2178] In 2011, several regulations were made and promulgated under the authority of EPOCA.

EPOCA was enacted with three fundamental objectives.[2179] First, is to address the challenges posed by modern technologies, especially the convergence of technologies. Second, is to harmonise and consolidate communication laws in order to overcome regular conflicts in their implementation, and third, to introduce the Central Equipment Identification Register (CEIR) and registration of SIM cards. The Act has nine parts. Part I covers preliminary provisions. This part has three sections providing for the name of the Act, its commencement date and application as well as interpretation of key terms and phrases. Part II is titled Electronic Communications. It has twenty eight sections. It governs licensing, interconnection and access issues. Part III bears the title Postal Communications. It has also twenty eight sections. This part regulates all matters pertaining to provision of postal services. Part IV deals with competition issues and conduct. This part is the longest of all. It has fifty five sections. The most prominent part in Part IV covers sections 84 to 102 which deal with the establishment of CEIR and registration of SIM cards. The reason is that this sub-part introduces significant development in the communications sector in Tanzania. Part V deals with enforcement issues. It has only two provisions. Part VI is the next longest part. It has forty four sections. This part deals with offences and penalties under EPOCA. However of particular importance are sections 118,120-124, 125-137, and 152 which touch upon electronic communications generally and specifically SIM cards. Part VII deals with miscellaneous provisions. It has seven sections. Part VIII deals with transitional matters with only one section and Part IX deals with amendments and repeals. It has eighteen sections.

EPOCA places obligation on every person who owns or intends to use mobile telephone in Tanzania to register his or her SIM card.[2180] At the same time it places obligation on every service provider to obtain information from buyers of SIM cards which identify them before activating

[2178] EPOCA 2010, s. 168(2).
[2179] Electronic and Postal Communications Bill, 2009, 'Objects and Reasons' at p.115.
[2180] EPOCA 2010, s.93(1). However it is doubtful if this obligation extends to persons who had acquired SIM cards prior to the coming into force of EPOCA. This is because on the 1st July 2009 when registration of SIM cards in Tanzania commenced, there was no legal obligation in its support. TCRA only issued a public notice requiring all service providers to register SIM-cards for their subscribers. Part of this notice reads, '...Pre-paid subscribers who have up to now not been registered shall be registered by their respective telecommunication service providers within a period of six months from 1st July 2009...With effect from 1st July, 2009 any new pre-paid subscribers shall be registered by their respective telecommunication service providers as soon as they start using a new SIM-card...Appropriate legislation is in the process through which registration of every person desiring to own and use a SIM-card shall be mandatory.' Worse still, EPOCA has no provision for the retrospective operation of the Act in order to take into account previous registered and unregistered SIM cards.

such cards in their networks.[2181] The list of information that a potential subscriber must give to the service provider on his or her identity include: in case of a natural person, full name of the potential subscriber, identity card number or any other document which proves identity of the potential subscriber, and residential, business or registered physical address, whichever is applicable.[2182] In case of a legal person, certificate of registration or incorporation, business license, Tax Payers Identification Number Certificate and where applicable the Value Added Tax will be required for registration purposes.[2183] In addition, a service provider may obtain 'any other information' from potential subscribers where it deems necessary.[2184] In effecting registration, a service provider is put under obligation to verify all the information from a potential subscriber before he or she proceeds to register him or her.[2185] Once registered, the information obtained from a potential subscriber will be retained in hard copies of documents or electronically.[2186] Where the information is obtained on behalf of a service provider, such person who acted on behalf is obliged to submit such information to the service provider in every fifteen days.[2187] A service provider, on the other hand, is required to submit all subscribers' information collected by himself or herself together with those by its agents to TCRA once in every month.[2188] The latter preserves this information in the subscribers' database.[2189]

As alluded to, once personal information is collected in a database a person from whom such information was collected has significantly less control over his or her personal information. This loss of control over ones personal information leads to lack of potential subscriber's knowledge of data flows and blacklisting. Probably to prevent this, section 98 of EPOCA casts duty on service providers to ensure that the information collected from subscribers is kept secure, confidential and not tampered with. This section states, 'a person who is a member, employee of application service licensee, or its agent, shall have a duty of confidentiality of any information received in accordance with the provisions of this Act.'[2190] It further provides, 'no person shall

[2181] EPOCA 2010, ss. 93(2) and 94(1).
[2182] Ibid, s. 93(2) (a).
[2183] Ibid, s. 93(2) (b).
[2184] Ibid, s. 93(2) (c).
[2185] Ibid, s. 93(3) (b); practically no verification has ever been done prior to registration of SIM card. Stakeholders raised concern over lack of National IDs in the registration process, see, Daily News, 27th June 2010, p.3,as such subscribers would come with various sorts of identification cards and got registered. It is therefore doubtful if the information submitted was accurate in the first place. This, in my view, will still complicate the ability of the database to trace criminals because of the possibility of false information with which criminals might have been registered.
[2186] EPOCA 2010, s. 93(4).
[2187] Ibid, s. 95.
[2188] Ibid, s. 91(3).
[2189] Ibid, ss. 91(1) and 91(2).
[2190] Ibid, s. 98(1).

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.'[2191]

From the above provision, it is clear that section 98 applies only to three categories of persons: a member, employee and an agent of a service licensee.[2192] Moreover, the duty of confidentiality imposed under this provision is limited to 'any information' received in accordance with the provisions of EPOCA. Unfortunately, the phrase 'any information' as used in section 98(1) of EPOCA is not defined. However, viewed narrowly, the information referred here may be relating to the identity of a subscriber which was submitted by a subscriber and obtained by a service provider during registration of SIM cards. This is because, when reading sections 93 and 94 of EPOCA, reference is only made to this type of information. However, when one reads section 98(1) in conjunction with section 98(2), which prohibits disclosure of the 'content of information' of any customer received in accordance with the provision of EPOCA, it definitely appears that the phrase 'any information' as used in section 98(1) is broad enough to encompass 'content of information'. The latter is sometimes referred to as 'content of communication'. Section 3 of EPOCA defines the term 'content' as information in the form of speech or other sound, data, text or images whether still or moving, except where transmitted in private communications. This type of information is not the one submitted during registration of SIM cards but the actual messages or conversations transmitted over service providers' networks when one makes a call to another person. One could therefore argue that EPOCA is an interception law as it authorises interception of subscribers' content of communication. This is so because it could be illogical for the Act to prohibit disclosure of the content of information which was not intercepted and retained it in the first place.

As pointed out, section 98(2) of EPOCA permits discloser of content of communication where persons who disclose such information are authorised by 'any other written law'. The phrase 'any other written law' is open ended.

Besides the interception and disclosure of information under 'any other written law' clause, EPOCA itself authorises interception and disclosure of communication. Section 99 states, 'a person shall not disclose any information received or obtained in exercising his powers or performing his duties in terms of this Act except - (a) where the information is required by any

[2191] Ibid, s. 98 (2).

[2192] Under sections 91(1) and 91(2) of EPOCA, TCRA is also a custodian of the subscribers' information, yet there is no provision in EPOCA which places upon it duty of confidentiality. Although such duty may be implied under section 99 of EPOCA, it is not adequate to bring TCRA within its ambit.

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.' As it can be noted from this provision, the ground for interception and subsequent disclosure of communication is only the need of such information by a law enforcement agency, court of law or tribunal. There are no other criteria. In effect therefore, when there is no specific provision in 'any other written law' authorising a person to intercept and retain the content of communication or other type of personal information, such person may still fulfil the requirements of section 98(2) by resorting to section 99 of EPOCA. He or she can just come forward and tell the service provider he or she wants certain information relating to a specific person by merely introducing himself or herself that he or she is a police officer carrying out investigation related to that person. Assessed from the constitutional right to privacy in Article 16 of the Tanzanian Constitution, it obviously appears that, section 99 of EPOCA fails to pass the proportionality test. This is because, the provision does not safeguard in any way subscribers' personal information held in the subscribers' database. Moreover, no one is placed in a position to scrutinise whether the need for intercepted information is justifiable in any way. Because of this, subscribers' personal information is unsecured. Moreover, their communication can be intercepted at any time without any appropriate remedy. Although EPOCA makes it an offence for unauthorised person to intercept and disclose any information,[2193] or for an authorised person having intercepted such communication to unlawfully disclose,[2194] it is difficult to enforce these provisions given the broadly and loosely drafting of sections 98 and 99 of EPOCA.

[2193] Section 120 of EPOCA states, '120, Any person who, without lawful authority under this Act or any other written law- (a) intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept any communications; or (b) discloses, or attempts to disclose to any other person the contents of any communications, knowingly or having reason to believe that the information was obtained through the interception of any communications in contravention of this section; or (c) uses, or attempts to use the contents of any communications, knowingly having reason to believe that the information was obtained through the interception of any communications in contravention of this section, commits an offence and shall, on conviction, be liable to a fine of not less than five million Tanzanian shillings or to imprisonment for a term not less than twelve months, or to both.'

[2194] Section 121 of EPOCA states, '121(1), Any person who is authorized under this Act intentionally discloses, or attempts to disclose, to any other person the contents of any communications, intercepted by means authorized by this Act- (a) knowing or having reason to believe that the information was obtained through the interception of such communications in connection with a criminal investigation; (b) having obtained or received the information in connection with a criminal investigation; or (c) improperly obstructs, impedes, or interferes with a duly authorized criminal investigation, commits an offence and shall, on conviction, be liable to a fine of not less than five million

7.4.3 Prevention of Terrorism Act 2002

The Prevention of Terrorism Act authorises interception of communication. [2195] Section 31 of this Act empowers a police officer to intercept communications in connection with investigation of terrorist offences.[2196] [2197] However before such police officer intercepts communication he must apply *ex parte* to the High Court of Tanzania[2198] and obtain a warrant of interception of communications order. A police officer may only make an application for interception of communication order with prior consent of the Attorney General.[2199] The High Court if is satisfied that there are reasonable grounds to believe that material information relating to the commission of a terrorist offence or the whereabouts of a suspect of terrorist offence is contained in that communication or communications of that descriptions, it may make an order requiring a service provider to intercept and retain specified communication(s) received or transmitted, or about to be received or transmitted by the service provider.[2200] Alternatively, the Court may authorise the police officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication(s), and subsequently to remove and retain it.[2201] While section 31 of the Prevention of Terrorism Act seems to have fulfilled the procedural requirement of Article 16(2) of the Tanzanian Constitution, it is doubtful if the same has satisfied the proportionality test under Article 30(2) of this Constitution. This is because, for example, section 31 does not put a limitation period for the order which the High Court may grant. Because of this, a person who is a target of the said interception may find his communication intercepted throughout under the justification of an interception order of the High Court even if such investigation fails to reveal any material information linking such person with the alleged terrorist offence. Apart from that, this section is silent on what will happen to the communication tapped by the police officer if it is not sufficient to warrant prosecution of the suspected person.

Tanzanian shillings or to imprisonment for a term not less than twelve months, or to both. (2) It shall be lawful under this Act for an officer, employee or agent of any network facilities provider, network service provider, application service provider or content service provider whose facilities or services are used in communications, to intercept, disclose, or use those communications in the normal course of his employment while engaged in any activity which is a necessary incident to the performance of his facilities or services or to the protection of the rights or property of the provider of the facilities or services, but the provider shall not utilize the facilities or services for observing or random monitoring unless it is for mechanical or service quality control or checks.'

[2195] Act. No.21 of 2002.

[2196] In this context, a police officer means a police officer of or above the rank of Assistant Superintendent, an immigration officer or a member of Tanzania Intelligence Security Service, see, section 28(2) of the Prevention of Terrorism Act, 2002.

[2197] What constitutes terrorist offences; see section 4 of the Prevention of Terrorism Act, 2002.

[2198] The Prevention of Terrorism Act 2002, s. 31(1).

[2199] Ibid, s.31(2).

[2200] Ibid, s.31(3) (a).

[2201] Ibid, s.31(3) (b).

7.4.4 Tanzania Intelligence and Security Service Act 1996

The Tanzania Intelligence and Security Service Act is another legislation which authorises interception of communication.[2202] Section 15(1) of this Act empowers the Tanzania Intelligence and Security Service (TISS) to investigate any person or body of persons whom or which it has reasonable cause to consider a risk or a source of risk of a threat to the state security. In the course of investigation TISS can institute surveillance of any person or category of persons.[2203] It is worth noting that the Tanzania Intelligence and Security Service Act contains the term 'intercept' in the definition section but the term is not found in any other provision of the Act. According to section 3, the word 'intercept' means that in relation to any communication not otherwise lawfully obtainable by the person making the interception, includes hear, listen to, record, monitor, or acquire the communication, or acquire its substance, meaning or purport. And the word 'interception' has a corresponding meaning to the word 'intercept'. However, the Act uses the term 'surveillance' in its substantive provisions instead of 'interception'. Unfortunately, the former term is not defined in the definition section of the Act. However the term simply means monitoring of the behaviour, activities, or other changing information, usually of people and often in a surreptitious manner.[2204] The former includes interception of electronically transmitted information.[2205] It is arguable that although the Tanzania Intelligence and Security Service Act has avoided using the term interception, it still authorises interception under the umbrella of surveillance. Moreover, since under section 28(2) of the Prevention of Terrorism Act a police officer also includes a member of the Tanzania Intelligence Security Service, the latter may still enforce interception under that law. Be as it may, the Tanzania Intelligence and Security Service Act, when measured against the provision of Article 16 of the Tanzanian Constitution, falls below the constitutional protection of the right to privacy. This is because, the Act does not prescribe any procedure for such interception. The interception is warrantless. Moreover, this Act broadly and loosely defines grounds for authorising interception. It simply provides state security as a blanket ground for interception.

[2202] Cap. 406 R.E 2002.
[2203]Ibid, ss. 5(1) (d) and (2) (b).
[2204] See, http://en.wikipedia.org/wiki/Surveillance last visited 1/05/2012.
[2205] Ibid

7.4.5 HIV and AIDS (Prevention and Control) Act 2008

The HIV/Aids Act applies in the context of HIV/Aids. It criminalises certain conducts and practices by health practitioners. One of such conducts is subjecting individuals into HIV test without their consent or knowledge.[2206] It is important to underline that under section 15(7) of the HIV and AIDS (Prevention and Control) Act 2008, consent and knowledge are distinct and separate criteria for establishing criminal liability. This is because the word 'or' has been used between the expressions 'compels any person to undergo HIV testing' and 'procures HIV testing to another person without the knowledge'. However it is doubtful if mere knowledge of HIV test on the part of individuals may be sufficient to justify HIV testing by health practitioners and exonerate them from criminal liability. This is because, individuals may have knowledge of HIV testing to which they are subjected yet they may still have not consented to such testing. It is arguable that since consent to HIV testing presupposes prior knowledge and understanding of all elements and implications of the examinations by individuals as well as agreement to be tested then the criterion of knowledge is subsumed into the criterion of consent and the two are inseparable. Moreover knowledge of HIV testing as such by individuals lacks the element of agreement to be tested, hence any HIV testing, even though procured with their knowledge, amounts to HIV testing without informed consent.

7.4.6 Regulations and Identification of Persons Act 1986

Since the end of 2011, Tanzania had started to register and issue national identification cards (National IDs) to citizens and residents. All matters relating to national IDs are governed by the Regulation and Identification of Persons Act 1986.[2207] This Act places an obligation on officers working in the agency not to disclose information collected from individuals for purposes of registration except under strict conditions provided by the law itself.[2208] This provision is not sufficient to protect individuals' personal information in the national ID database.

[2206] See Section 15(7) of the HIV and AIDS (Prevention and Control) Act 2008(Act No. 28 of 2008) which states, ' Any health practitioner who compels any person to undergo HIV testing or procures HIV testing to another person without the knowledge of that other person commits an offence'.
[2207] Act No. 11 of 1986.
[2208] Ibid, s.29.

7.4.7 Human DNA Regulation Act 2009

The DNA Act[2209] regulates the collection, packing, transportation, storage, analysis and disposal of sample for human DNA as well as disclosure of genetic information and research. The Act incorporates in its part IV (ss.23-37) provisions governing collection and analysis of sample for human DNA. It further incorporates provisions governing disclosure of information on human DNA in part VIII (ss.52-65). These provisions are not likely to be sufficient in protecting privacy in an environment which has no general right of protection of the right to privacy.[2210]

7.5 Conclusion

Privacy is a constitutional right in Tanzania. It is further entrenched in various statues albeit not comprehensively. It has also been shown that there is a gradual growth of concerns for privacy in Tanzania. This is partly because of the diminishing impact of *Ujamaa* ideology. At present there are no debates or discussions for the adoption of comprehensive data privacy law. This is despite the fact that Tanzania is a part of the East African Community which has adopted recommendations for its members to put in place legal mechanisms for regulating and protecting personal data. It is premature to predict the effect of the SADC Data Protection Framework and the AU Cyber Convention on Tanzania, once they are adopted. Similarly, the government has yet felt compelled by the requirements of Article 25 of Directive 95/46/EC to provide an 'adequate' standard for protection of personal data in its legal system. Presumably, the exceptions provided in Article 26 of the Directive 95/46/EC are currently working smoothly for Tanzania.

[2209] Act No.8 of 2009.
[2210] See e.g., Ubena, J., 'Privacy: A Forgotten Right in Tanzania', the Tanzania Lawyer, 2012, Vol.1, No.2, pp. 72-114.

8. Comparative Conclusions

8.1 Key Findings

The analyses comprised in the previous chapters have shown that data privacy is an international policy issue. The broad agenda saved by such policy and concomitantly data privacy regulations are mainly two: to afford individuals with protection of the right to privacy and to promote flow of information across nations in order to achieve economic objectives. Initially, data privacy issues were prominently considered an affair of the most individualised societies of America and Europe. This is probably because the discourse of data privacy originated there at the time when American and European societies had already transformed to that stage. The dominant literature asserts that beyond America and Europe, where societies are largely collectivist, there is no culture of privacy. As a result, the absence of data privacy legislation in those parts of the world has been regarded as an empirical evidence to support such literature. The present study has undertaken to investigate the state of privacy in sub-Saharan Africa with particular focus in the three case studies: Mauritius, South Africa and Tanzania. Three specific research questions were formulated:-

a) Does a well-defined concept or value to privacy exist in sub-Saharan Africa?

b) To what extent is privacy protected in sub-Saharan Africa? Do such means of protection reflect the pre-existing values of privacy in the sub-continent?

c) Is the emerging regime of data privacy law in sub-Saharan Africa which most invariably is styled in European Data Protection Directive 95/46/EC, a mere compliance to meet the 'adequacy' standard set by such law for non-European countries rather than a genuine attempt to ensure respect to individuals' privacy in sub-Saharan Africa?

In investigating the above research questions, this thesis employed a hybrid method. As pointed out in paragraph 1.2.4 of this thesis, such methods included doctrinal, empirical and international comparative legal research.

As indicated in paragraph 4.3.3, this study has found that there is neither concept nor theory which defines the notion of privacy in sub-Saharan Africa. Calls for attempts to define privacy in the context of African culture particularly in Uganda has yet resulted to any of such definitions.

Yet, it has been found that, in Africa, privacy is understood almost the same way as it is the case in the Western individualist culture. Neethling's theory of privacy, postulated in the context of South Africa, appears as the only attempt to define privacy in Africa. However, such definition is derived from the Western individualist theories. As alluded to, Neethling's theory falls under the class of information control theory covered in paragraph 2.3.1 of this thesis. Since Neethling's theory of privacy has been cited with approval by the South African courts and at the same time it has been frequently cited by commentators in different parts of Africa without almost any objection, there is little chance for a specific definition that will define privacy in terms of collective culture to develop.

However, despite the lack of a privacy concept, values to privacy are evolving in different parts of Africa. As pointed out in chapter 4, particularly in paragraph 4.3, values to privacy in Africa have been largely externally influenced. Further in paragraph 4.3.1 of the thesis, it has been revealed that specific factors termed as 'determinants of privacy concerns in Africa' have worked in manners that make Africans attach weight on privacy issues. These factors have been further considered in the three specific cases in chapters 5, 6 and 7. Generally considered, the neo-liberal ideologies that became dominant through SAPs have far reaching implications towards Africans' values to privacy. These have significantly transformed the economic, political, social and cultural foundations of Africans.

It is imperative to mention that, some African countries' values to privacy have been nourished by long history of persecutions and injustice. This study has revealed in chapter 6 that in South Africa, *apartheid* has nourished to a large extent concerns for privacy making privacy a relatively high value compared to other places in Africa. Conversely, *Ujamaa* ideology in Tanzania has greatly made individuals to share even the most sensitive information without being aware of the potential risks arising out of such sharing. Yet in Mauritius, the relatively higher penetration of ICTs has somewhat alerted individuals of the associated privacy risks. In contrast, in Nigeria, the prevalence of fraud scams have made individuals keen not to disclose personal information, including bank card details, to unknown persons over the Internet.

It is submitted that, the dominant discourse based on 'culture of collectivism' as an explaining factor for the state of privacy in Africa is a generalised normative assumption which obscures concrete factual situations and specifics. Moreover, the fact that at some point such discourse takes cognisance of the emerging trend of adoption of data privacy legislation in Africa without

offering any explanation renders it problematic. This is because the dominant discourse takes 'individualism' as a pre-condition for the development of values to privacy.

This study has also found that prior to the adoption of Directive 95/46/EC; there was no any African country with comprehensive data privacy legislation. It has been shown in chapters 3 and 4 that at that time there were three international data privacy policies influencing national data privacy legislation: Council of Europe *Convention 108*; *OECD Guidelines* and *UN Guidelines*. The last two policies are non-binding. This means that the Convention was the only international binding data privacy policy prior to Directive 95/46/EC. Yet, its influence was severely limited because of lack of provisions that would regulate flow of information from a party to a non-party state. In other words, the Convention did not contain equivalent provisions as Articles 25 and 26 of the Directive. Similarly, the U.S Self-Regulatory scheme had limited application. Its influence did not go far. Thus it can generally be submitted that previous international data privacy policies exerted little influence in the global development of privacy policies and regulations.

However, this study has revealed in paragraphs 1.2.1 and 4.4 that, at national level, the dominant form of privacy protection in Africa was and still it is the constitutional right to privacy. This form of protection can not generally be regarded as a direct response to privacy concerns in African countries. It rather came about as a result of the independence constitutions which were largely prepared by the colonial masters on behalf of the people in African colonies. There is consensus among commentators that the Bill of Right in which the right to privacy is embedded, was incorporated in the independence constitutions in order to protect the interests of settlers who remained in the colonies after independence. Admittedly, at this juncture, claim for privacy were virtually absent. However some African countries' independence constitutions, such as those in Kenya and Zimbabwe, did not incorporate express provisions for privacy although they had Bills of Right. Tanzania completely rejected a Bill of Right in its independence constitution. She incorporated it in its 1977 Constitution later in 1984 following SAPs' conditionalities. In 2010, Kenya adopted a new constitution with an express provision of privacy. In the same vein, Zimbabwe is currently considering a new constitution with an express provision on protection of privacy. This is also the case with South Africa, whose 1994 and 1996 Constitutions expressly contain the right to privacy. The latter three cases suggest that the constitutional right to privacy in those countries were adopted as a result of demands by citizens. Yet, it may be argued that those provisions were merely incorporated in these constitutions as compliance to the

international standards in the international human treaties. However, the South African Constitution 1996 has been the basis of the development of a fairly large body of case law on constitutional right to privacy. This suggests that although a constitutional right to privacy was not adopted as a response to concerns of privacy in many African countries, this system of protection increasingly provides a remedy for violations of privacy.

Apart from constitutional protection, there are protections of privacy in statutes particularly in the communications sector. Other sectors with limited protection include the health sector particularly the medical confidentiality; penal laws, etc. Similarly, these were incorporated into the legal systems of African countries as a result of compliance to international standards. For example, the medical confidentiality is a requirement from international law and the *Hippocratic Oath* for the medical professionals.

At the same time, privacy has long been protected under common law even before the adoption of the Directive 95/46/EC. South Africa is the only African country which has been protecting privacy through the common law tort of *delict*. The first landmark case is *O'Keeffe*. Decided in 1954, *O'Keeffe* established for the first time an independent right to privacy in South African legal system. This was subsequently incorporated in the Constitution of South Africa in 1994 and later 1996. Today, in South Africa, privacy is protected both under the common law and section 14 of the South African Constitution 1996.

It has also been found that the eleven data privacy enactments in Africa were all adopted after 2000. This was the time the Directive 95/46/EC had already come into operation. Previous chapters, particularly chapters 4, 5 and 6 have found that the adoption of data protection in Africa is largely a response to comply with Articles 25 and 26 of the Directive. The primary agenda behind this adoption is to achieve economic motives. Protection of individuals' privacy in these countries appears only as a secondary agenda. Mauritius and South Africa present strong empirical evidence in support of this finding. In both cases the *travaux préparatoires* clearly indicate that the adoption of data privacy legislation is geared towards supporting the IT Enabled Services and Business Process Outsourcing sectors. Yet, in South Africa, the protection of privacy is also contemplated probably because of two other factors: the fact that the common law and constitutional protection can not sufficiently apply in the field of processing of personal data and also the country's long history of the injustice of the *apartheid* regime. The accreditation

request for the EU rating by Mauritius and the intention to do so by South Africa, supports further the above finding.

Yet, it has also been shown in the previous chapters that although Cape Verde was the first country in Africa to adopt data privacy legislation in 2001 it has not established the office of the data protection commissioner. This is similar to Seychelles. The latter adopted its data privacy legislation in 2003, hence becoming the second African country to adopt data privacy legislation. However, until the time of writing this thesis, Seychelles had not promulgated its law. It can be submitted that the Cape Verdean and Seychelles' data privacy legislation are assets for these countries which await the right opportunity to be utilised. Similarly, a realistic interpretation is that these pieces of legislation were adopted as a response to the requirements of the Directive. The fact that such laws have remained unimplemented for about a decade since they were enacted, partly refutes any claim that their existence was largely a response to Africans' concerns for privacy in the respective countries.

It has also been shown in the previous discussions and analyses particularly in chapters 4, 5 and 6 that the emerging data privacy legislation in Africa inhere significant disparities. This is partly due to various factors such as a country's legal system and tradition; lack of a regional data privacy regime; multiplicities of uncoordinated sub-regional data privacy frameworks; and the needs of a particular country. For instance, although Mauritius has comprehensive data privacy legislation and South Africa has a Bill on such law, the two have significant different scopes. While South Africa proposes a Bill whose protection extends to juristic persons, Mauritian data privacy law protects only the natural living person. South Africa's approach is based on the long recognition of protection of privacy of juristic person under its common law. Moreover, the South African Bill on data privacy law incorporates a special regime of protection of personal data of children while Mauritian law does not specifically provide such protection. The regime of international transfer of personal data is significantly different too. While the Mauritian law is premised on the 'adequacy' standard similar to the EU Directive 95/46/EC, the South African Bill is premised on lower standard applicable when a foreign country fails to pass the 'adequacy standard'. In other words, the Mauritian data privacy law is based on both Articles 25 and 26 of the EU Directive, while that of South Africa is only based on Article 26. The justification advanced in the *travaux préparatoires* of the South African Bill on data privacy is that, since South Africa has a large share of investments in other African countries, adopting the 'adequacy' standard would prejudice her investment interests in those jurisdictions which have not implemented comprehensive data

protection legislation. At the same time South Africa feels that by adopting an international regime of transfer of personal data based on Article 26, it will sufficiently meet the standards set by the European regime. On the other hand, Mauritius targets European investments as a result of which, adoption of a stronger 'adequacy' standard is necessary to guarantee and assure investors that Mauritius will not be a 'data haven'. There are also notable differences on the data protection authorities in the two jurisdictions. Previous analyses in chapters 5 and 6 clearly indicate that the South African Bill contains more elaborative provisions which guarantee the independence of the data protection commissioner and the staff under him or her. This is different from similar provisions in the Mauritian law. It can be noted from the *travaux préparatoires* that right from the beginning, the Mauritian executive wanted to have a strong control of the commissioner of data protection. And in fact, the original Data Protection Act 2004 in Mauritius incorporated a regime which empowered the prime minister to give direction to the commissioner in discharge of his or her statutory duties. The law was only amended in 2009 in an attempt to seek EU adequacy rating. This is not the case for South Africa. Probably because of the experience of *apartheid*, the Bill has strong protection of the commissioner. For similar reasons, the legislative processes of the data privacy legislation in the two countries are sharply different. The data protection legislation in Mauritius was adopted nearly in a week's time and without public consultation. On the other hand, the South African Bill has passed through extensive public consultations. The legislation has been on agenda since mid-1990s, yet up to now it has not been adopted.

There are also other statutes protecting privacy in Africa. However some of them were largely influenced by the September 11 attacks in the United States. For example, the regime of interception of communications incorporated in the terrorism Acts or general communications Acts are aimed to control crimes rather than to regulate data processing as such. Some limited provisions relating to privacy are similarly incorporated in the freedom of information Acts in some African countries.

Another important notable trend is the increasingly adoption of data privacy frameworks at sub-regional and regional level in Africa. Chapter 4 indicates the adoption of such frameworks in the AU, EAC, ECOWAS, and SADC. Although all of them have been largely influenced by the EU Directive 95/46/EC, they have different scope. Their nature is also different. Some frameworks are binding while others are not. It is imperative to point that, the influence of such frameworks to the development of data privacy law in Africa is yet to be noted. For example, since it was

adopted in 2010, the ECOWAS data privacy framework has not exerted any significant impact to the adoption of data privacy law in the sub-region. The countries with data privacy legislation in ECOWAS appear to have adopted such law prior to the ECOWAS framework. Similarly, the EAC Cyber Law Frameworks which are largely recommendations have not yet influenced the development of data privacy law in the sub-region.

The disparities of privacy standards in different national laws, sub-regional and regional level in Africa are bound to produce far reaching consequences. For example, in a long run the cross-jurisdiction transfer of personal data will increasingly become difficult. Moreover, the problem of lack of harmonisation is likely to occur. This will in turn result in both strong and weak system of protection of individuals' personal data.

The general observation which can be made here is that there is little or no direct link between the level of privacy concerns and the system of privacy and data protection in Africa. The latter had arisen almost independently from Africans' concerns for privacy. Despite that, such systems of privacy protection and more particularly the constitutional right to privacy have provided the legal foundations for data privacy legislation in Africa.

Finally, it can be concluded that privacy is gradually becoming an important value in Africa. This is largely due to the interplay of many factors particularly those explained in chapter 4. Although, the emerging data privacy legislation in Africa is much influenced by the requirements of the Directive 95/46/EC, particularly Articles 25 and 26 suggesting that such laws exist largely to support European interests in Africa, Africans in their respective countries rely on them to obtain remedies for breach of their privacy. For example, the seven complaints filed and decided by the Commissioner of Data Protection in Mauritius concerned Mauritian citizens. At the same time, while such laws were not largely enacted in response to particular privacy concerns in Africa, they are potentially capable of influencing such concerns particularly when citizens in African countries increasingly become aware of their rights.

8.2 Future Research Agenda

The present study, although has been undertaken on Africa particularly in sub-Saharan Africa, it has special focus on Mauritius, South Africa and Tanzania. While the findings in these three cases are somewhat similar in many respects, there are notable significant dissimilarities. For this reason, these cases may not be replicated in some other African countries with specific different

conditions without difficulties. Based on this account, specific research studies are needed to understand for example, the state and protection of privacy in the North African countries which this study excluded due to the peculiarities of the Arab and Islamic cultures. Similarly, as the present study is a general one, more specific research studies in various sectors (e.g. communications, health, employment, biometric, et cetera) are needed in order to supplement general data privacy legislation with specific ones, codes of conduct and guidelines. Other areas which warrant research studies include privacy on the Internet in the African context; HIV/Aids context, etc.

9. Bibliography

A. Books and Journal Articles

6, P., The Future of Privacy: Private Life and Public Policy, Vol.1, DEMOS, London, 1998.

Achebe, C., Things Fall Apart, East African Educational Publishers, Nairobi/Kampala/Dar es Salaam, 1966.

Adams, A.A *et al.*, 'The Japanese Sense of Information Privacy', Al & Society, 2009, Vol.24, No.4, pp.327-341.

African Business., 'Urbanisation for Better or for Worse' December 2011, Issue No.381, pp.17-24.

Ahmad, N., 'A Study of Individual Freedom and Religious Liberalism in Islamic Jurisprudence', the Journal Jurisprudence, 2009, pp.41-66.

Akonumbo, A.N., 'HIV/AIDS Law and Policy in Cameroon: Overview and Challenges,' African Human Rights Law Journal, 2006, Vol.6, No.1, pp. 85-122.

Aldhouse, F., 'The Transfer of Personal Data to Third Countries under EU Directive 95/46/EC', International Review of Law Computers & Technology, 1999, Vol.13, No.1, pp.75-79.

Alemna, A.A and Sam, J., 'Critical Issues in Information and Communication Technologies for Rural Development in Ghana', Information Development 2006, Vol.22, No.4, pp.236-241.

Aliber, M and Walker, C., 'The Impact of HIV/AIDS on Land Rights: Perspectives from Kenya', World Development, 2006, Vol.34, No.4, pp.704-727.

Allagui, I., 'The Arab Spring and the Role of ICTs: Editorial Introduction', International Journal of Communication, 2011, Vol.5, pp.1435-1442.

Allan, K and Currie, I., 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa', South Africa Journal on Human Rights, 2007, Vol. 23, No.3, pp. 563-579.

Allen, A.L., Uneasy Access: Privacy for Women in a Free Society, Rowman & Littlefield, Totowa, NJ, 1988.

Alonso, C *et al.*, 'ECJ Decision on Spain has Europe-wide Implications', Privacy Laws & Business International Report, 2011, No.114, pp.1,6-7.

Andrew, H., 'The "Westminster Model" Constitution Overseas: Transplantation, Adaptation and Development in Commonwealth States', Oxford University Commonwealth Law Journal, 2004, Vol.4, No.2, pp.143-166.

Anglewicz, P and Chintsanya, J., 'Disclosure of HIV Status between Spouses in Rural Malawi', AIDS Care: Psychological and Sicio-Medical Aspects of AIDS/HIV, 2011, Vol.23, No.8, pp.998-1005.

Arisaka, Y., 'Beyond "East" and "West": Nishida's Universalism and Postcolonial Critique', The Review of Politics, 1997, Vol.59, No.3, pp. 541-560.

Arostegui, H.T., 'Defining "Private Life" Under Article 8 of the European Convention on Human Rights by Referring to Reasonable Expectations of Privacy and Personal Choice', California Western International Law Journal, 2005, Vol.35, No.2, pp.153-202.

Arzt, D.E., 'The Application of International Human Rights Law in Islamic States', Human rights Quarterly, 1990, Vol.12, No.2, pp.202-230.

Azmi, I.M., 'Personal Data Protection Law: the Malaysian Experience', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.125-135.

Bakari, M and Makulilo, A., 'Beyond Polarity in Zanzibar? The "Silent" Referendum and the Government of National Unity', Journal of Contemporary African Studies, 2012, Vol.30, No.2, pp.195-218.

Baldwin, J and Davis, G., 'Empirical Research in Law' in P.Cane and M. Tushnet (eds), The Oxford Handbook of Legal Studies, Oxford University Press, 2003.

Banisar, D., 'Linking ICTs, The Right to Privacy, Freedom of Expression and Access to Information', East African Journal of Peace & Human Rights, 2010, Vol.16, No.1, pp.124-154.

Banisar, D., 'Privacy and Data Protection Around the World', Conference Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13th September 1999, pp.1-5.

Banisar, D., 'The Right to Information and Privacy: Balancing Rights and Managing Conflicts', Working Paper, The International Bank of Reconstruction and Development/The World Bank, 2011.

Banisar, D., 'Data Protection Laws around the World Map', papers.ssrn.com (accessed 20/12/2011).

Banjo, A., 'The ECOWAS Court and the Politics of Access to Justice in West Africa', CODESRIA Africa Development, 2007, Vol.32, No.1, pp.69-87.

Barnes, S.B., 'A Privacy Paradox: Social Networking in the United States', First Monday, 2006, Vol.11, No.9, firstmonday.org (accessed 3/10/2011).

Basu, S., 'Policy-Making, Technology and Privacy in India', The Indian Journal of Law and Technology, 2010, Vol.6, pp.65-88.

Bell, D.A., East Meets West: Human Rights and Democracy in East Asia, Princeton University Press, Princeton, 2000.

Bennett, C. J., Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, Ithaca/London, 1992.

Bezanson, R.P., 'The Right to Privacy Revisited: Privacy, News and Social Change 1890-1990', California Law Review, 1992, Vol.80, No.5, pp.1133-1175.

Bing, J., 'Data Protection, Jurisdiction and the Choice of Law', Privacy Law & Policy Reporter, 1999, Vol. 6, No. 6, pp. 92-98.

Bing, J., 'The Council of Europe Convention and the OECD Guidelines on Data Protection', Michigan Yearbook of International Legal Studies, 1984, Vol.5, pp.271-304.

Bing, J., 'The identification of applicable law and liability with regard to the use of protected material in the digital context', ECLIP Research Report, 2000, pp.236-258.

Birnhack, M. D., 'The EU Data Protection Directive: An Engine of a Global Regime', Computer Law & Security Report, 2008, Vol.24, No.6, pp.508-520.

Blume, P., 'Data Protection in the Private Sector', Scandinavian Studies in Law, 2004, Vol.47, pp.297-318.

Blume, P., 'Data Protection of Law Offenders', Information, Communication and Society, 1998, Vol.1, No.4, pp.442-466.

Blume, P., 'Privacy as a Theoretical and Practical Concept', International Review of Law Computers & Technology, 1997, Vol.11, No.2, pp.193-202.

Blume, P., 'Transborder Data Flow: Is there a solution in sight?', International Journal of Law and International Technology, 2000, Vol.8, No.1, pp.65-86.

Bonde, J.P., From EU Constitution to Lisbon Treaty, Foundation for EU Democracy and the EU Democrats in cooperation with Group for Independence and Democracy in the European Union, www.eudemocrats.org (accessed 20/12/2011).

Bonnici, J.P.M., 'Recent European union Developments on Data Protection...in the Name of Islam or "Combating Terrorism"', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.161-175.

Booth, S *et al.*, 'What are "Personal Data"?' A Study conducted for the UK Information Commissioner, University of Sheffield, 2004.

Bradshaw, S *et al.*, 'Contracts for clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', International Journal of Law and Information technology, 2011, Vol.19, No.3, pp. 187-223.

Brennan, J.R., 'Blood Enemies: Exploitation under Urban Citizenship in the Nationalist Political Thought of Tanzania, 1958-75', Journal of African History, 2006, Vol.47, No.3, pp.389-413.

Bridge, J.W., 'Judicial Review in Mauritius and the Continuing Influence of English Law', International and Comparative Law Quarterly, 1997, Vol.46, No.4, pp.787-811.

Briggs, J., 'Villagisation and the 1974-6 Economic Crisis in Tanzania', The Journal of Modern African Studies, 1979, Vol.17, No.4, pp.695-702.

Brown, L. N., 'Mauritius: Mixed Laws in a Mini-Jurisdiction', in Örücü, E (eds), et al., Studies in Legal Systems: Mixed and Mixing, Kluwer International, London, 1996, pp.210-214.

Bulford, C., 'Between East and West: The APEC Privacy Framework and the Balance of International Data Flows', I/S: A Journal of Law and Policy for the Information Society, 2008, Vol.3, No.3, pp.705-722.

Burchell, J., 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid', Electronic Journal of Comparative Law, 2009, Vol. 13, No.1, pp.1-26.

Burdon, M and Telford, P., 'The Conceptual Basis of Personal Information in Australian Privacy Law, eLaw Journal: Murdoch University Electronic Journal of Law, 2010, Vol.17, No.1, pp.1-27.

Burgos, C and Pavón, B., 'Spanish Supreme Court provides Limited Relief for Data', Computer Law & Security Review, 2011, Vol.27, No. 1, pp.83-85.

Burns, K and Hutchinson, T., 'The Impact of "Empirical Facts" on Legal Scholarship and Legal Research Training', the Law Teacher, 2009, Vol.43, No.2, pp.166-168.

Butchner, B and Kang, J., 'Privacy in Atlantis', Harvard Journal of Law & Technology, 2004, Vol. 18, No.1, pp.229-267.

Bygrave, L. A, 'The Place of Privacy in Data Protection Law' University of New South Wales Law Journal, 2001, Vol. 24, No. 1, pp. 277-283.

Bygrave, L. A., 'Privacy Protection in a Global Context – A Comparative Overview', Scandinavian Studies in Law, 2004, Vol. 47, pp. 319–348.

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

Bygrave, L.A., 'A Right to Privacy for Corporations? *Lenah* in International Context', Privacy Law & Policy Reporter, 2001, Vol.8, pp.130-134.

Bygrave, L.A., 'Data Protection Pursuant to the Right in Human Rights Treaties', International Journal of Law and Information Technology, 1998, Vol.6, No.3, pp.247-284.

Bygrave, L.A., 'Data Protection Reforms in Scandinavia', Privacy Law & Policy Reporter, 1998, Vol.5, pp.9-12.

Bygrave, L.A., 'Determining Applicable Law pursuant to European Data Protection Legislation', Computer Law & Security Report, 2000, Vol.16, No. 4, pp.252-257.

Bygrave, L.A., 'International Agreements to Protect Personal Data' in G.Greenleaf and J.B. Rule(eds)., Global Privacy Protection: The First Generation, Edward Elgar Publishing Limited, Cheltenham,UK/Northampton, MA,USA, 2008, pp.15-49.

Bygrave, L.A., 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', Computer Law & Security Report, 2001, Vol.17, No.1, pp.17-24.

Bygrave, L.A., 'Privacy and Data Protection in an International Perspective', Scandinavian Studies in Law, 2010, Vol. 56, pp.165-200.

Byrnes, R.M(ed)., South Africa: A Country Study, GPO for the Library of Congress, Washington, 1996.

Canadian Institutes of Health Research (CIHR)., 'Selected International Legal Norms on the Protection of Personal Information in Health Research', December, 2001.

Cannataci, J.A and Bonnici, J.P.M., 'Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty', Information & Communications Technology Law, 2005, Vol.14, No.1, pp.5-15.

Cannataci, J.A., 'Privacy, Technology Law and Religions across Cultures', Journal of Information, Law and Technology, 2009, Vol.1, pp. 1-22.

Capurro, R., 'Information Ethics for and from Africa', International Review of Information Ethics, 2007, Vol.7, No.9, pp.1-13.

Capurro, R., 'Privacy: An Intercultural Perspective', Ethics and Information Technology, 2005, Vol.7, No.1, pp.37-47.

Carauna, M.M and Cannataci, J.A., 'European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.99-124.

Carrim, A.J., 'Use and Standardisation of Mauritian Creole in Electronically Mediated Communication', Journal of Computer-Mediated Communication, 2009, Vol.14, No.3, pp.484-508.

Carrim, A.R., 'Language Use and Attitudes in Mauritius on the Basis of the 2000 Population Census', Journal of Multilingual and Multicultural Development, 2005, Vol. 26, No.4, pp.317-332.

Casola, V *et al.*, 'Access Control in Cloud-on-Grid Systems: The *Perf*Cloud Case Study', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp. 427-444.

Chakraborty, S., 'Mobile Phones Bridging the Information Divide Issues and Lessons from Africa', JOMC223.

Chaligha, A *et al.*, 'Uncritical Citizens or Patient Trustees? Tanzanians' Views of Political and Economic Reform', Afrobarometer Paper No.18, 2002.

Chalton, S., 'The Court of Appeal's Interpretation of "Personal Data" in Durant v. FSA-a Welcome Clarification, or a Cat amongst the Data Protection Pigeons?', Computer Law & Security Report, 2004, Vol.20, No.3, pp. 175-181.

Cheung, A.S.Y., 'China Internet going wild: Cyber-hunting versus Privacy Protection', Computer Law & Security Review, 2009, Vol. 25, pp. 275-279.

Chofor Che, C.A., 'Challenges of Incorporating and Enforcing a Bill of Rights in the Cameroonian Constitution', Cameroon Journal on Democracy and Human Rights, 2008, Vol.2, No.1, 2008, pp. 68-72.

Chrimes, S.B., 'Counting as Citizens: Recognition of the Nubians in the 2009 Kenyan Census', Ethnopolitics, 2011, Vol.10, No.2, pp.205-218.

Chui, W.H and McConville, M (eds)., Research Methods for Law, Edinburgh University Press, 2010.

Church, J. *et al*., Human Rights from a Comparative and International Law Perspective, UNISA Press, Pretoria, 2007.

Church, J., 'The Place of Indigenous Law in a Mixed Legal System and a Society in Transformation: A South African Experience', ANZLH E-Journal, 2005, pp.94-106.

Church, P and Cumbley, R., 'What is Personal Data? The House of Lords identifies the Issues-Common Services Agency v. Scottish Information Commissioner [2008] UKHL 47', Computer Law & Security Report, 2008, Vol. 24, No. 6, pp. 565-567.

Clarke, R., 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century', Xamax Consultancy Pty Ltd, 2000, pp.1-38.

Clarke, R., 'Information Technology and Datavaillance', Communications of ACM, 1988, Vol. 31, No. 5, pp. 498-512.

Connelly, A.M., 'Problems of Interpretation of Article 8 of the European Convention on Human Rights', International and Comparative Law Quarterly, 1986, Vol.35, pp.567-593.

Connolly, C., 'Asia-Pacific Region at the Privacy Crossroads', World Data Protection Report, 2008, Vol.8, No.9, pp.8-16.

Cooper, D.M., 'Transborder Data Flow and the Protection of Privacy: The Harmonization of Data Protection Law', Fletcher Forum, 1984, Vol.8, No.2, pp.335-352.

Cottrell, R.C., South Africa: A State of Apartheid, Chelsea House Publishers, Philadelphia-U.S.A, 2005.

Crook, J.R., 'The International Court of Justice and Human Rights', Northwestern University Journal of International Human Rights, 2004, Vol.1, pp.1-8.

Crowder, M., 'Indirect Rule-French and British Style', Africa: Journal of the International African Institute, 1964, Vol.34, No.3, pp. 197-205.

Cuijpers, C., 'A Private Law Approach to Privacy: Mandatory Law Obliged?', SCRIPTed, 2007, Vol.4, No.4, pp.304-318.

Currie, I and Klaaren, J., Commentary on the Promotion of Access to Information Act, *Siber* Ink, South Africa, 2002.

Currie, I., 'The Concept of Privacy in the South African Constitution: Reprise', Journal of South African Law, 2008, Vol.2008, No. 3, pp.549-557.

Currie, I., 'The Protection of Personal Information Act and its Impact on Freedom of Information', University of the Witwatersrand, Johannesburg, www.opendemocracy.org.za (accessed 27/09/2011).

Dann, P., 'Thoughts on a Methodology of European Constitutional Law', German Law Journal, 2005, Vol. 6, No. 11, pp.1461-1467.

Davis, F., 'What do We mean by "Right to Privacy"?' San Dakota Law Review, 1959, Vol.4, pp.1-24.

Davis, S., 'Is there a Right to Privacy?', Pacific Philosophical Quarterly, 2009, Vol. 90, No.4, pp.450-475.

De Hert, P and Gutwirth, S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action', in Gutwirth, S *et al* (eds)., Reinventing Data Protection?, Springer, 2009, pp.3-44.

De Hert, P and Schreuders, E., 'The Relevance of Convention 108', 33,42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19-20, November, 2001.

Deighton, J., 'The Right to be Let Alone', Journal of Interactive Marketing, 1998, Vol.12, N0.2, pp.2-4.

Dhillon, G and Kolkowska, E., 'Can a Cloud Be Really Secure? A Socratic Dialogue', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp.345-360.

Di Fabio, D., 'The European Constitutional Treaty: An Analysis', German Law Journal, 2004, Vol.5, No.8, pp.945-956.

Dobinson, I and Johns, F., 'Qualitative Legal Research' in W.H Chui and M. McConville (eds)., Research Methods for Law, Edinburgh University Press, 2010.

Drzemczewski, A., 'The European Human Rights Convention: Protocol No. 11 Entry into Force and First Year of Application', Documentação e Direito Comparado, 1999, nos 79/80, pp.219-247.

Dwasi, J.A., The Human Right to Work in the Era of HIV and AIDS, Law Africa, Nairobi/Dar es Salaam/Uganda, 2009.

Eden, J.M., 'When Big Brother Privatizes: Commercial Surveillance, the Privacy Act, 1974, and the Future of RFID', Duke Law & Technology Review, 2005, No.20, pp.1-24.

Edwards, C.P and Whiting, B.B (eds)., NGECHA: A Kenyan Village in a Time of Rapid Social Change, University of Nebraska Press, Lincoln/London, 2004.

Elahi, S., 'Privacy and Consent in the Digital Era', Information Security Technical Report, 2009, Vol.14, No.3, pp.113-118.

Electronic Privacy Information Centre and Privacy International (PI), 'Overview of Privacy' in Privacy and Human Rights Report, 2006.

Elgesem, D., 'The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data', Ethics and Information Technology, 1999, Vol.1, No.4, pp.283-293.

Ellger, R., Der Datenschutz im grenzüberschreitende Datenverkehr: eine rechtsvergleichende und kollisions-rechtliche Untersuchung, Baden-Baden: Nomos, 1990.

Engels, F., The Origin of the Family, Private Property and the State, International Publishers Co. Inc., New York, 1942.

Epstein, L and King, G., 'Empirical Research and the Goals of Legal Scholarship: The Rules of Inference', University of Chicago Law Review, 2002, Vol.69, No.1, pp.1-133.

Ergas, Z., 'Why Did the Ujamaa Village Policy Fail?-Towards a Global Analysis', The Journal of Modern African Studies, 1980, Vol.18, No.3, pp.387-410.

Evrensel, A., 'Introduction', in Evrensel, A(ed)., Voter Registration in Africa: A Comparative Analysis, Electoral Institute for the Sustainability of Democracy in Africa(EISA), Johannesburg, 2010, pp.1-54.

Ezedike, E.U., 'Individualism and Community Consciousness in Contemporary Africa: A Complementary Reflection', Sophia: An African Journal of Philosophy, 2005, Vol.8, No.1, pp.59-64.

Farrell, H., 'Negotiating Privacy across Areanas: The EU-US "Safe Harbor" Discussions' in Héritier, A(ed)., Common Goods: Reinventing European and International Governance, Rawman & Littlefield, Boulder/New York/Oxford, 2002, pp.101-123.

Ferreira, C., 'The Europeanization of Law' in Oliveira, J and Cardinal, P(eds)., One Country, Two Systems, Three Legal Orders-Perspective of Evolution: Essays on Macau's Autonomy after the Resumption of Sovereignty by China, Springer-Verlag, Berlin/Heidelberg, 2009, pp.171-190.

Fishman, W.L., 'Introduction to Transborder Data Flows', Stanford Journal of International Law, 1980, Vol16, pp.1-26.

Floridi, L., 'Four Challenges for a Theory of Informational Privacy', Ethics and Information Technology, 2006, Vol.8, No.3, pp.109-119.

Ford, P., 'Implementing the Data Protection Directive - An Outside Perspective', Privacy Law & Policy Reporter, 2003, Vol. 9, pp. 141-149.

Foye, S., 'Book Review on Understanding Privacy by Daniel J.Solove', Journal of High Technology Law, 2008-2009.

Fried, C., 'Privacy', Yale Law Journal, 1968, Vol.77, pp.475-493.

Froomkin, A. M., 'The Death of Privacy?', Stanford Law Review, 2000, Vol.52, No.5 pp. 1461-1543.

Frowein, J.A and Wolfrum, R(eds)., 'Domestic Implementation of the International Covenant on Civil and Political rights to its article 2 para.2', Max Plunk Yearbook of United Nations Law, 2001, Vol.5, pp.399-472.

Fuchs, C and Horak, E., 'Africa and the Digital Divide', Telematics and Informatics, 2008, Vol.25, No.2, pp.99-116.

Gavison, R., 'Privacy and the Limits of the Law', Yale Law Journal, 1980, Vol.89, No.3, pp.421-471.

Gayrel, C., 'Data Protection in the Arab Spring: Tunisia and Morocco', Privacy Laws & Business International Report, 2012, No.115, pp.18-20.

Gayrel, C., 'Mauritius: Data Protection in an Evolving Island Economy', Privacy Laws & Business International Report, 2011, No.114, pp.20-22.

Gebremichael, M.D and Jackson, J.W., 'Bridging the gap in Sub-Saharan Africa: A holistic look at information poverty and the region's digital divide', Government Information Quarterly 2006, Vol. 23, No.2, pp.267-280.

Gellman, R and Dixon, P., 'The History of failed Self-Regulation in the United States', Privacy Laws & Business International Report, 2011, No.114, pp.10-12.

Goodsell, E.E., 'Constitution, Custom, and Creed: Balancing Human Rights Concerns with Cultural and Religious Freedom in Today's South Africa', Brigham Young University (BYU) Journal of Public Law, 2007, Vol.21, No.1, pp.109-152.

Goodsell, E.E., 'Constitution, Custom, and Creed: Balancing Human Rights Concerns with Cultural and Religious Freedom in Today's South Africa', Brigham Young University (BYU) Journal of Public Law, 2006, Vol.21, No.1, pp.109-152.

Greenleaf G., 'APEC's Privacy Framework: A new low standard', Privacy Law & Policy Reporter, 2005, Vol. 11, pp.121-124.

Greenleaf, G and Bygrave, L.A., 'Note entirely adequate but far away: Lessons from how Europe sees New Zealand data protection', Privacy Laws & Business International Report, 2011, No.111, pp.8-9.

Greenleaf, G *et al.*, 'Interpreting the Security Principle', Working Paper No.1, v.6 March 2007, pp.1-37.

Greenleaf, G., 'The Global Trajectory of Data Privacy Laws', SCRIPT Seminar, Edinburgh, 8 December 2011, pp.1-13.

Greenleaf, G., '76 Global Data Privacy Laws', [2011] UNSWLRS 36.

Greenleaf, G., 'APEC Privacy Principles Version 2 - Not quite so Lite, and NZ wants OECD full strength', Privacy Law & Policy Reporter, 2003, Vol. 10, pp. 45-49.

Greenleaf, G., 'APEC Privacy Principles: More Lite with every version', Privacy Law & Policy Reporter, 2003, Vol.10, pp. 105-111.

Greenleaf, G., 'Asia-Pacific Data Privacy: 2011, Year of Revolution?', University of New South Wales, Faculty of Law Research Series, 2011, Paper No.29, pp.1-17.

Greenleaf, G., 'Asia-Pacific Developments in Information Privacy Law and Its Interpretation', New Zealand Privacy Issues Forum, 2006, pp.1-25, at pp5-6.

Greenleaf, G., 'Australia's APEC Privacy Initiative: The Pros and Cons of "OECD Lite"' Privacy Law & Policy Reporter, 2003, Vol.10, pp. 1-6.

Greenleaf, G., 'Criticisms of the APEC Privacy Principles (Version 9), and recommendations for improvements', Working Paper, March 2004.

Greenleaf, G., 'Do not dismiss "Adequacy": European Standards entrenched', Privacy Laws & Business International Report, 2011, No.114, pp.16-18.

Greenleaf, G., 'Global Data Privacy Laws: 89 Countries, and Accelerating', Privacy Laws & Business International Report, Special Supplement, 2012, No.115.

Greenleaf, G., 'Global Data Privacy Laws: Forty Years of Acceleration', Privacy Laws & Business International Report, 2011, No. 112, pp. 11-17.

Greenleaf, G., 'Independence of Data Privacy Authorities (Part I): International Standards', Computer & Security Review, 2012, Vol.28, No.1, pp.3-13.

Greenleaf, G., 'Safe Harbor's Low Benchmark for "adequacy": EU sells out Privacy for US$', Privacy Law & Policy Reporter, 2000, Vol. 7, No.3, pp.45-49.

Greenleaf, G., 'The APEC Privacy Initiative:"OECD Lite" for the Asia-Pacific?', Privacy Laws & Business, 2004, Vol.71, pp. 16-18.

Greenleaf, G., 'The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108', International Data Privacy Law, 2012, Vol.2, No.2, pp.68-92.

Gross, H., 'The Concept of Privacy', New York University Law Review, 1967, Vol.42, No.1, pp.34-54.

Grundlingh, L., 'Government Responses to HIV/AIDS in South Africa as Reported in the Media, 1983-1994', South African Historical Journal, 2001, Vol.45, No.1, pp.124-154.

Gunasekara, G., 'The "Final" Privacy Frontier? Regulating Trans-Border Data Flows', International Journal of Law and Information Technology, 2007, Vol.17, No.2, pp. 142-179.

Gupta, A., 'The Role of Knowledge Flows in Bridging North-South Technological Divides: A case analysis of biotechnology in Indian agriculture', Centre for Science, Policy, and Outcomes, Washington, 2003.

Gutwirth, S., Privacy and the Information Age, Lanham/Boulder/New York/Oxford/ Rowman & Littlefield Publ., 2002.

Gyekye, K., The Unexamined Life: Philosophy and the African Experience, Ghana University Press, Accra, 1988.

Hahlo, H.R and Kahn, E., The South African Legal System and Its Background, Juta, Cape Town, 1968.

Hammitt, H., 'A Constitutional Right of Informational Privacy', Government Technology, 1998.

Hansungule, M., 'Independence of the Judiciary and Human Rights Protection in Southern Africa', pp.1-9, www.pdfcari.com (accessed 29/03/2012).

Hayat, M.A., 'Privacy and Islam: From the Quran to Data Protection in Pakistan', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.137-148.

Heeney, C and Weigand, H., 'Privacy Protection and Communicative Respect', Proceedings of the 8th International Working Conference on the Language-Action Perspective on Communication Modelling (LAP), Tilburg, the Netherlands, 2003.

Heinz Klug., Constitutional Democracy: Law, Globalism and South Africa's Political Reconstruction, Cambridge University Press, 2000.

Heisenberg, D., Negotiating privacy: the European Union, the United States, and personal data protection, Boulder/Colo. : Lynne Rienner Publishers, 2005.

Hellsten, S.K., 'Human Rights in Africa: From Communitarian Values to Utilitarian Practice', Human Rights Review, March-April, 2004.

Hemeson, C.J., 'Directive on Consumer Data for SIM Card Registration in the Telecommunications Sector: An African Perspective', Social Science Research Network, 2012, pp.1-12.

Hey, E. and Mak, E., 'Introduction: The Possibilities of Comparative Law Methods for Research on the Rule of Law in a Global Context', Erasmus Law Review, 2009, Vol. 2, No. 3, pp.1-3.

Hijmans, H and Scirocco, A., 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?', Common Market Law Review, 2009, Vol.46, pp.1485-1525.

Hilberg, R., The Destruction of the European Jew, Holmes & Meier Publishers, New York, 1985.

Hilhosrst, S., 'Remmy Ongala: Capitalist Transition and Popular Music in Tanzania 1979-2002', Journal of African Cultural Studies, 2009, Vol.21, No.2, pp.105-126.

Hinz, M.O., 'Human Rights between Universalism and Cultural Relativism? The Need for Anthropological Jurisprudence in the Globalising World', in A.Bösl and J.Diescho (eds)., Human Rights in Africa: Legal Perspectives on their Protection and Promotion, Macmillan Education Namibia, 2009, pp. 3-32.

Hirji, K.F., 'Socialism Yesterday' in Hirji, K. F(ed)., CHECHE: Reminiscences of a Radical Magazine, Mkuki na Nyota, Dar es Salaam, 2010, pp.134-154.

Hobby, S.P., 'The EU Data Protection Directive: Implementing a Worldwide Data Protection Regime and How the U.S Position has progressed', International Law & Management Review, 2005, Vol. 1, pp.155-190.

Hodgkinson, D and Wright, T., 'Johnson v The MDU: "Processing" under the DPA', e-Commerce Law & policy, 2007, Vol.9, No.5, pp.1-4.

Hondius, F.W., 'Data Law in Europe', Stanford Journal of International Law, 1980, Vol.16, pp.87-111.

Hornby, A.S., Oxford Advanced Learner's Dictionary of Current English, 7th Edition, Oxford University Press, New York, 2005.

Hörner, S., 'Datenschutz und Kriminalitätsprävention in Südafrika Ein Vergleich mit Deutschland am Beispiel der Einführung der Videoüberwachung öffentlicher Plätze', KAS-AI 11/04, S.62-88.

Hornung, G and Schnabel, C., 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination', Computer Law and Security Report, 2009, Vol.25, No.1, pp.84-88.

Howard, P.N., The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam, Oxford University Press, Ney York, 2010.

Hutton, L., 'Looking Beneath the Cloak: An Analysis of Intelligence Governance in South Africa', Institute for Security Studies (ISS), 2007, Paper No. 154, pp.1-24.

Inness, J.C., Privacy, Intimacy and Isolation, Oxford University Press, New York, 1992.

Izuogu, C.E., 'Data Protection and Other Implications in the Ongoing SIM Card Registration Process', 2010, papers.ssrn.com (accessed 11/10/2011).

Jagessar, U and Sedgwick, V., 'When is Personal Data not "Personal Data"-The Impact of Durant v. FSA.', Computer Law & Security Report, 2005, Vol.21, No. 6, pp.505-511.

Joseph, K.J., 'Transforming Digital Divide into Digital Dividend: South-South Cooperation in Information-Communication Technologies', Cooperation South, 2005, pp.102-124.

Kaduuli, S.C., 'To Tap or Not to Tap? This is the Uganda Phone Question', WIRETAPPING: REGULATORY PERSPECTIVES, Ramakistaisah Jilla, ed., Hyderabad, India: Icfai University Press, 2010, pp.209-219.

Kantarcioglu, M and Clifton, C., 'Assuring Privacy when Big Brother is Watching', DMKD03:8th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery, 2003.

Kasusse, M., 'Bridging the Digital Divide in Sub-Saharan Africa: The Rural Challenge in Uganda', The International Information & Library Review, 2205, Vol.37, No.3, pp.147-158.

Katunzi, J., 'Managing Change in Tanzania Public Enterprises: Swallowing Bitter Pills', The IFM Journal of Finance and Management, 1998, Vol.6, No.2, pp.14-23.

Keeva, S., 'The Threat of Unrest: Traditions Provide Hope for Stability', ABA Journal, 1994, Vol.80, No.4, pp.50-60.

Keevy, I., '*Ubuntu* versus the Core Values of the South African Constitution', Journal for Juridical Science, 2009, Vol. 34, No.2, pp.19-58.

Kennedy, G *et al*., 'Data Protection in the Asia-Pacific Region', Computer Law & Security Review, 2009, Vol.25, No.1, pp.59-68.

Khan, N.M and Emmambokus, N., 'Customer Adoption of Internet Banking in Mauritius', International Journal of Business Research and Management(IJBRM), 2011, Vol.2, No.2, pp.53-58.

Kiekbaev, D.I., 'Comparative Law: Method, Science or Educational Discipline?', Electronic Journal of Comparative Law, 2003, Vol. 7.3, www.ejcl.org(accessed 27/09/2011).

Kigongo, J.K., 'The Concept of Individuality and Social Cohesion: A Perversion of Two African Cultural Realities' in Dalfovo, A.T *et al* (eds)., The Foundations of Social Life: Uganda Philosophical Studies, I, The Council for Research in Values and Philosophy, Washington, 1992, pp.59-68.

Kimani, P., 'When the family becomes a burden', Daily Nations, Weekender Magazine, 23 January 1998.

King, R.U., 'Healing Psychological Trauma in the Midst of Truth Commission: The Case of *Gacaca* in Post-Genocide Rwanda', University of Toronto Press Journals, 2011, Vol.6, No.2, pp.134-151.

Kirby, M., 'Information Security-OECD Initiatives', Journal of Law and Information Science, 1992, Vol.3, No.1, pp.25-46.

Kirby, M., 'Legal Aspects of Transborder Data Flows', Global Telecommunications Congress and Exhibition, Vancuvouver BC Canada, 25 October 1990, Inter Comm, 90, pp.1-23.

Kirby, M., 'Legal Aspects of Transborder Data Flows', International Computer Law Adviser, 1991, Vol.5, No.5, pp.4-11.

Kirby, M., 'Privacy Protection-A New Beginning?', Prometheus, 2000, Vol.18,No.2, pp.125-132.

Kirby, M., 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy', International Privacy Law, 2011, Vol.1, No.1, pp.6-14.

Knoll, M., 'Budget Support: A Reformed Approach or Old Wine in New Skins?' UNCTAD Discussion Papers, No. 190, October 2008, pp. 1-13.

Kong, L., 'Enacting China's Data Protection Act', International Journal of Law and Information Technology, 2010, Vol.18, No.3, pp.197-226.

Kong, L., 'Data Protection and Transborder Data Flow in the European and Global Context', The European Journal of International Law (EJIL), 2010, Vol. 21, No.2, pp.441-456.

Kuan Hon, W *et al.*, 'The Problem of "Personal Data" in Cloud Computing: What information is regulated?-the Cloud of Unknowing', International Data Privacy Law, 2011, Vol.1, No.4, pp.211-228.

Kuhlen, R., Informationsethik. Umgang mit Wissen und Information in elektonischen Räumen.UTB: Universitätsverlag Konstanz, Konstanz 2004 cited in Capurro, R., 'Privacy: An Intercultural Perspective', Ethics and Information Technology, 2005, Vol.7, No.1, pp.37-47.

Kuner, C *et al.*, 'The Intricacies of Independence', International Data Privacy Law, 2012, Vol.2, No.1, pp.1-2.

Kuner, C., 'An International Legal Framework for Data Protection: Issues and Prospects', Computer Law & Security Review, 2009, Vol.25, pp.307-317.

Kuner, C., 'Data Protection Law and International Jurisdiction on the Internet (Part 2)', International Journal of Law and Information Technology, 2010, Vol.18, No.3, pp.227-247.

Kuner, C., 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future', TILT Law & Technology Working Paper No. 016/2010 October 2010, Version: 1.0, p.6, Social Science Research Network Electronic Paper Collection

Kuner, C., 'Table of Data Protection and Privacy Law Instruments Regulating Transborder Data Flows', Annex to the study 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future', TILT Law & Technology, Social Science Research Network Electronic Paper Collection.

Kusamotu, A., 'Privacy Law and Technology in Nigeria: The Legal Framework will not meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/46', Information & Communications Technology Law, 2007, Vol.16, No. 2, pp. 149 – 159.

Lassiter, J.E., 'African Culture and Personality: Bad Social Science, Effective Social Activism, Or a Call to Reinvent Ethnology?', African Studies Quarterly, 2000, Vol.3, No.3, pp.1-21.

Lawson, C., 'Japan's New Privacy Act in Context', UNSW Law Journal, 2006, Vol.29, No.2, pp.88-113.

Levy, P.I., 'Sanctions on South Africa: What Did They Do', Discussion Paper, No. 796, Yale University, 1999, pp.1-13.

Lindsay, D., 'Misunderstanding "Personal Information": Durant v Financial Services Authority', Privacy Law & Policy Reporter, 2004, Vol.10, No.10, www.austlii.edu.au(accessed 03/11/2011).

Linkomises, L., 'EU regulation planned to harmonise national laws', Privacy Laws & Business International Report, 2011, No. 114, pp. 1, 3-4.

Lipset, S.M., 'Pacific Divide: American Exceptionalism-Japanese Uniqueness', International Journal of Public Opinion Research, 1993, Vol.5, No. 2, pp.121-166.

Litman, J., 'Information Privacy/Information Property', Stanford Law Review, 2000, Vol. 52, pp.1283-1313.

Liver, A., On Privacy, Forthcoming from Routledge (November 2011), www.alever.net(accessed 12/11/2011).

Lofchie, M., 'Agrarian Crisis and Economic Liberalisation in Tanzania', The Journal of Modern African Studies, 1978, Vol.16, No.3, pp.451-475.

Long, W.J and Quek, M.P., 'Personal Data Privacy Protection in an Age of Globalisation: the US-EU Safe Harbor Compromises', Journal of European Public Policy, 2002, Vol.9, No.3, pp.325-344.

Loubser, M *et al*., The Law of *Delict* in South Africa, Oxford University Press Southern Africa, Cape Town, 2010.

Louw, J., 'Culture and Self in South Africa: Individualism-Collectivism Predictions', The Journal of Social Psychology, 2000, Vol.140, No.2, pp.210-217.

MacDonald, D.A., '*Ubuntu* bashing: the marketisation of "African values" in South Africa', Review in South African Political Economy, 2010, Vol.37, No.124, pp.139-152.

Maduagwu, M.O., 'Globalization and Its Challenges to National Culture and Values: A Perspective from Sub-Saharan Africa', in Köchler, H(ed)., Globality versus Democracy? The Changing Nature of International Relations in the Era of Globalization, Jamahir Society for Culture and Philosophy, Vienna, 2000, pp.213-224.

Mahadeo, S.K., 'English Language Teaching in Mauritius: A Need for clarity of vision regarding English Language Policy', International Journal of Language, Society and Culture, 2006, Issue No.18, www.educ.utas.edu.au (accessed 17/03/2012).

Mahadeo, S.K., 'History of English and French in Mauritius: A Study in Language and Power', International Journal of Language, Society and Culture, 2004, Issue No.14,

Makgoro, J.Y., '*Ubuntu* and the Law in South Africa', Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, 1998, Vol. 1, No. 1, pp.1-11.

Makulilo, A.B., 'Registration of SIM Cards in Tanzania: A Critical Evaluation of the Electronic and Postal Communications Act, 2010', Computer and Telecommunications Law Review (CTLR), 2011, Vol. 17, No. 2, pp.48-54.

Makulilo, A.B., 'You must take medical test: Do Employers intrude into Prospective Employees' Privacy?' Datenschutz und Datensicherheit (DuD), 8/2010, pp.571-575.

Makulilo, A.B., Tanzania: A De Facto One Party State?, VDM Verlag Dr. Müller Aktiengesellschaft & Co. KG, Germany, 2008.

Mancuso, S., 'Legal Transplants and Economic Development: Civil Law vs. Common Law?' in Oliveira, J and Cardinal, P(eds)., One Country, Two Systems, Three Legal Orders-Perspective of Evolution: Essays on Macau's Autonomy after the Resumption of Sovereignty by China, Springer-Verlag, Berlin/Heidelberg, 2009, pp.75-90.

Marchini, R and Tebbut, K., 'European Data Protection Authorities Provide New Guidance on "Personal Data"', A Legal Update from Dechert's Data Protection and Privacy Group, July, 2007, No.3, www.dechert.com (accessed 3/11/2011).

Margulis, S.T., 'Privacy as a Social Issue and Behavioral Concept', Journal of Social Issue, 2003, Vol.59, No.2, pp.24-261.

Martin, B., 'The Information Society and the Digital Divide: Some North-South Comparisons', International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2005, Vol. 1, No. 4, pp. 30-41.

Martin, R., Personal Freedom and the Law in Tanzania: A Study of Socialist State Administration, Oxford University Press, Nairobi/Dar es Salaam/ Lusaka/ Addis Ababa, 1974.

Martin, W., 'Trade Policies, Developing Countries and Globalisation', Development Research Group, World Bank, 9 October 2001, pp.1-35.

Maurer, S., 'Genetic Identity in Mauritius', Antrocom, 2010, Vol.6, No.1, pp.53-62.

May, B.E *et al.*, 'The Differences of Regulatory Models and Internet Regulation in the European Union and the United States', Information & Communications Technology Law, 2004, Vol.13, No.3, pp.259-272.

Mayambala, K.R., 'Phone-Tapping & the Right to Privacy: A Comparison of the Right to Privacy in Communication in Uganda and Canada', BILETA, 2008.

Mbiti, J., African Religions and Philosophy, Heinemann, London, 1969.

Mbonu, N.C *et al.*, 'Stigma of People with HIV/AIDS in Sub-Saharan Africa: A Literature Review', Journal of Tropical Medicine, 2009, Article ID 145891, 14 pagesdoi:10.1155/2009/145891.

Mc Cullagh, K., 'A Study of Data Protection: Harmonisation or Confusion?', 21st Annual British & Irish Law, Education and Technology Association (BILETA) Conference 'Globalisation and Harmonisation in Technology Law' Malta, April, 2006.

McAllister, P., 'Ubuntu-Beyond Belief in South Africa', Sites: New Series, 2009, Vol.6, No.1, pp.1-10.

McBride, W.L., 'The Concept of Justice in Max, Engels, and Others', Ethics, 1975, Vol.85, No.3, pp.204-2018.

McCrea, R., 'Limitations on Religion in Liberal Democratic Polity: Christianity and Islam in the Public Order of the European Union', LSE Law, Society and Economy, Working papers 18/2007, Science Research Network library.

McDonald, D.A., 'Ubuntu Bashing: The Marketisation of "African Values" in South Africa', Review of African Political Economy, 2010, Vol. 37, No.124, pp.139-152.

Mcgrath, J.E., 'Methodology Matters: Doing Research in the Behavioural and Social Sciences', in R. M. Baecker *et al*., (eds), Readings in Human-Computer Interaction: Toward the Year 2000, Morgan Kaufmann Publishers, 1995.

McLuhan, M., The Gutenberg Galaxy, University of Toronto Press, 1962.

McQuoid-Mason, D.J., 'Privacy' in Chaskalson, M *et al*, (eds)., Constitutional Law of South Africa, Juta, Kenwyn, 1996.

Metz, H.C(ed)., Mauritius: A Country Study, GPO for the Library of Congress, Washington, 1994.

Mgaya, K., 'Development of Information Technology in Tanzania' in Drew, E.P and Foster, F.G (eds)., Information and Technology in Selected Countries: Reports from Ireland, Ethiopia, Nigeria and Tanzania, University of United Nations, Tokyo, 1994.

Moerel, L., 'Back to Basics: When does EU Data Protection Law apply?', International Data Privacy Law, 2011, Vol.1, No.2, pp. 92-110.

Moerel, L., 'The long arm of EU Data Protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by website worldwide?', International Data Privacy Law, 2011, Vol.1, No.1, pp.28-46.

Molla, A., 'Downloading or Uploading? The Information Economy and Africa's Current Status', Information Technology for Development, 2000, Vol.9, No.3 & 4, pp.205-221.

Moore, A., 'Defining Privacy', Journal of Social Philosophy, 2008, Vol. 39, No.3, pp.411-428.

Morjn, J., 'Balancing Fundamental Rights and Common Market Freedoms in Union Law: Schmidberger and Omega in the Light of the European Constitution', European Law Journal, 2006, Vol.12, No.1, pp.15-40.

Murata, K and Orito, Y., 'Privacy Protection in Japan: Cultural Influence on the Universal Value', Electronic Proceedings of Ethicomp, Linkoping, Sweden, 2005.

Murata, K and Orito, Y., 'Rethinking the Concept of Information Privacy: A Japanese Perspective', Electronic Proceedings of Ethicomp, Tokyo, Japan, 2007.

Murray, P.J., 'The Adequacy Standard under Directive 95/46/EC: Does U.S Data Protection Meet This Standard?', Fordham International Law, 1997, Vol. 21, No.3, pp.931-1018.

Murungi, M.M., 'Kenya's New Constitution sets New Standards for Privacy and Data Protection', January, 2010, michaelmurungi.blogspot.com (accessed 11/10/2011).

Murungi, M.M., Cyber Law in Kenya, Kluwer Law International, the Netherlands, 2011.

Nakada, M and Tamura, T., 'Japanese Conceptions of Privacy: An Intercultural Perspective', Ethics and Information Technology, 2005, Vol.7, pp.27-36.

Ncube, C.B, 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems', Journal of Information, Law and Technology, (JILT), 2004, No. 2, www2.warwick.ac.uk (accessed 9/10/2011).

Ncube, C.B., 'Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-surveillance in South Africa', SCRIPTed, 2006, Vol.3, No.4, pp.344-354.

Ndebele, P *et al.*, 'HIV/Aids reduces the relevance of the principle of individual medical confidentiality among the Bantu people of Southern Africa', Theoretical Medicine and Bioethics, 2008, Vol.29, No. 5, pp.331-340, p.331.

Neethling, J *et al.*, Neethling's Law of Personality, 2nd Edition, LexisNexis, Durban, 2005.

Neethling, J *et al.*, Neethling's Law of Personality, Butterworth, Durban, 1996.

Neethling, J., 'The Concept of Privacy in South African Law', The South African Law Journal, 2005, Vol.122, No.1, pp.18-28.

Neethling,J *et al.*, Neethling-Potgieter-Vesser Law of Delict, 6th Edition, LexisNexis, Durban, 2010.

Newell, S., 'Corresponding with the City: Self-help Literature in Urban West Africa', Journal of Postcolonial Writing, 2008, Vol.44, No.1, pp.15-27.

Norris, C *et al.*, 'Editorial: The Growth of CCTV: A Global Perspective on the International Diffusion of Video Surveillance in Public Accessible Space' Surveillance and Society, 2004, 2(2/3), pp.110-135.

Ntibagirirwa, S., 'A Wrong Way: From Being to Having in the African Value System' in Giddy, P(ed)., Protest and Engagement: Philosophy after Apartheid at an Historically Black South African University, South African Philosophical Studies, II, The Council for Research in Values and Philosophy, Washington, 2001, pp.65-81.

Nwauche, E.S., 'The Right to Privacy in Nigeria', Review of Nigerian Law and Practice, 2007, Vol.1, No.1, pp.62-90.

O'Donnell, M.K., 'New Dirty War Judgements in Argentina: National Courts and Domestic Prosecutions of International Human Rights Violations', New York University Law Review, 2009, Vol.84, pp.333-374.

Okigbo, P., 'Social Consequences of Economic Development in West Africa', The Annals of the American Academy of Political and Social Science, 1956, Vol.305, pp.125-133.

Olinger, H.N, *et al.*, 'Western privacy and/or Ubuntu? Some Critical Comments on the influences in the Forthcoming Data Privacy Bill in South Africa', the International Information & Library Review, 2007, Vol. 39, No. 1, pp. 31-43.

Olsson, A.R., 'Big Brother, Small Sisters and Free Speech: Reanalyzing some Threats on Personal Privacy', Scandinavian Studies in Law, 2004, Vol.47, pp.373-387.

Olutayo, A.O and Omobawale, A.O., 'Capitalism, Globalisation and the Underdevelopment Process in Africa: History in Perpetuity', African Development, 2007, Vol.32, No.2, pp.97-112.

Omobowale, A.O., 'The Youth and the Family in Transition in Nigeria', Review of Sociology, 2006, Vol.16, No.2, pp.85-95.

Oppong, R.F., 'Re-Examining International Law: An Examination of Recent Trends in the Reception of International Law into Legal Systems in Africa', Fordham International Law Journal, 2007, Vol.30, No.2, pp.296-345.

Orwell, G., 1984, Penguin Books, New York, 1972.

Papakonstantinou, V., 'A Data Protection Approach to Matching Operations among Public Bodies', International Journal of Law and Information Technology, 2001, Vol.9, No.1, pp. 39-64.

Parent, W.A., 'Privacy, Morality, and the Law', Philosophy & Public Affairs, 1983, Vol.12, No.4, pp.269-288.

Paul, J.C.N., 'Developing Constitutional Orders in Sub-Saharan Africa: An Unofficial Report', Third World Legal Studies, 1988, Vol.7, No.1, pp.1-34.

Pee, L.G *et al.*, 'Bridging the Digital Divide: Use of Public Internet Kiosks in Mauritius', Journal of Global Information Management (JGIM), 2010, Vol.18, No.1, pp.15-38.

Peter, C.M., 'The Enforcement of Fundamental Rights and Freedoms in Tanzania: Matching Theory and Practice', in P.M. Peter and I.H. Juma (eds), Fundamental Rights and Freedoms in Tanzania, Mkuki na Nyota, Dar es Salaam, 1998, pp.47-59.

Phinnemore, D., 'The Treaty Establishing a Constitution for Europe: An Overview', The Royal Institute of International Affairs, 2004, pp.1-23.

Pieters, W., 'Security and Privacy in the Clouds: A Bird's Eye View', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp. 445-457.

Piris, J.C., The Lisbon Treaty: A Legal and Political Analysis, Cambridge University Press, UK, 2010.

Posner, R.A., 'The Right of Privacy', Georgia Law Review, 1978, Vol. 12, No.3, pp.193-422.

Poullet, Y *et al*., 'Data Protection in Clouds', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp.377-409.

Prempeh, H.K., 'Africa's "Constitutionalism Revival": False start or new dawn?,' International Journal of Constitutional Law, 2007, Vol.5, pp.469-506.

Prins, J.E.J., 'The Propertization of Personal Data and Identities', Electronic Journal of Comparative Law, 2004, Vol.8, No.3, pp.1-7.

Quansah, E.K., 'An Examination of the Use of International Law as Interpretative Tool in Human Rights Litigation in Ghana and Botswana', in Killander, M(ed)., International Law and Domestic Human rights Litigation in Africa, Pretoria University Law Press(PULP), South Africa, 2010, pp.37-56.

Qvortrup, M., 'The Three Referendums on the European Constitutional Treaty in 2005', The Political Quarterly, 2006, Vol.77, No.1, pp.86-97.

Raab, C.D and Bennett, C.J., 'Protecting Privacy across Borders: European Policies and Prospects', Public Administration, 1994, Vol.72, pp.95-112.

Raab, C.D., 'Information Privacy: Networks of Regulation at the Sub-global Level', Global Policy, 2010, Vol.1, No.3, pp. 291-302.

Rawls, J., 'Justice as Fairness', The Philosophical Review, 1958, Vol.62, No.2, pp.164-194.

Rawls, J., A Theory of Justice, Revised Edition, Harvard University Press, 1971.

Reding, V., 'The Upcoming Data Protection Reform for the European Union', International Data Privacy Law, 2011, Vol.1, No.1, pp.3-5.

Reed, J. S., 'Human Rights in Tanzania', in Legum, C, and Mmari, G., (eds) Mwalimu: The Influence of Nyerere, London/Dar es Salaam/Treaton: James Currey/Mkuki na Nyota/ Africa World Press, 1995.

Regan, P., 'American Business and the European Data Protection Directive: Lobbying Strategies and Tactics', in Bennett, C and Grant, R (eds)., Visions of Privacy, University of Toronto Press, Toronto, 1999.

Reidenberg, J.R., 'Setting Standards for Fair Information Practices in the US Private Sector', Iowa Law Review, 1995, Vol. 80, No.3, pp.497-552.

Rempell, S., 'Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas', Florida Journal of International Law, 2006, Vol.18, pp. 807-842.

Riddell, B., 'Things Fall Apart Again: Structural Adjustment Programmes in Sub-Saharan Africa', The Journal of Modern African Studies, 1992, Vol.30, No.1, pp.53-68.

Rishmawi, M., 'The Arab Charter on Human Rights and the League of Arab States: An Update', Human Rights Law Review, 2010, vol.10, No.1, pp.169-178.

Rishmawi, M., 'The Revised Arab Charter on Human Rights: A Step Forward?', Human Rights Law Review, 2005, Vol.5, No.2, pp.361-376.

Ritchie, D., 'Is it Possible to define "Privacies" within the Law? Reflections on the "Securitisations" Debate and the Interception of Communications', International Review of Law, Computers & Technology, 2009, Vol.23, Nos.1-2, pp.25-34.

Rodney, W., How Europe Underdeveloped Africa, East African Educational Publishers, Nairobi/Kampala/Dar es Salaam, 1972.

Roe, E.M., 'Individualism versus Community in Africa? The Case of Botswana', The Journal of African Modern Studies, 1988, Vol.26, No.2, pp.347-350.

Roos, A., 'Data Protection Provisions in the Open Democracy Bill, 1997', Journal of Contemporary Roman-Dutch Law/Tydskrif Vir Hedendaagse Romein- Hollandse Reg (*THRHR*), 1998, Vol.61, No.3, pp.497-506.

Roos, A., 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position', South African Law Journal (SALJ), 2007, Vol.124, No. 2, pp.400-437.

Roos, A., 'Data Protection' in Dana, M., *et al*, Information and Communications Technology Law, LexisNexis, Durban, 2008, pp.313-397.

Roos, A., 'Personal Data Protection in New Zealand: Lessons for South Africa?', Potchefstroom Electronic Law Journal, 2008, Vol.8, No.4, pp.61-109.

Roos, M., 'Definition of the Problem: The Impossibility of Compliance with both European Union and United States', Transnational Law & Contemporary Problems, 2005, Vol.14, No.3, pp.1137-1162.

Ruiter, J and Warnier, M., 'Privacy Regulation for Cloud Computing: Compliance and Implementation in Theory and Practice', in Gutwirth, S *et al* (eds)., Computers, Privacy and Data Protection: an Element of Choice, Springer, Dordrecht/Heidelberg/London/New York, 2011, pp.361-376.

Sachs, D., 'A Fallacy in Plato's Republic', The Philosophical Review, 1963, Vol.72, No.2, pp.141-158.

Safier, S., 'Between Big Brother and the Bottom Line: Privacy in Cyberspace', Virginia Journal of Law and Technology, Spring, 2000, Vol. 5, No.6, www.vjolt.net (accessed 3/10/2011).

Salbu, S.R., 'The European Union Data Privacy Directive and International Relations', Vanderbilt Journal of Transnational Law, 2002, Vol.35, pp.655-595.

Salmer, K.S., '*Elekronisk databehandling og rettssamfunne*t', in *Forhandling ved Det 30. Nordiske juristmøtet, Oslo 15-17. august 1984*(Oslo: Det norske styret for De nordiske jurstmøter, 1984).

Salmon, J., 'Field Research in Sensitive Areas', Junior Research Group, 'Micropolitics of Armed Groups', Working Papers Micropolitics No. 1/2006.

Santon, G.H., 'Could the Rwandan Genocide have been prevented?', Journal of Genocide Research, 2004, Vol.6, No.2, pp.211-228.

Schermer, B.W., 'The Limits of Privacy in Automated Profiling and Data Mining', Computer Law & Security Review, 2011, Vol. 27, No.1, pp. 45-52.

Schoeman, F.D., Privacy and Social Freedom, Cambridge University Press, USA, 1992.

Schwartz, P.M and Reidenberg, J.R., Data Privacy Law: A Study of United States Data Protection, Michie Law Publishers, Charlottesville, 1996.

Schwartz, P.M., 'Privacy and Democracy in Cyberspace', Vanderbilt Law Review, 1999, Vol.52, pp.1609-1701.

Selmer, K.N., 'Council of Europe Convention on Automatic Data Processing', Medical Informatics, 1989, Vol.14, No.3, pp.211-214.

Senghor, L., 'Negritude' in Optima, 16:8, 1966 cited in Lassiter, J.E., 'African Culture and Personality: Bad Social Science, Effective Social Activism, Or a Call to Reinvent Ethnology?', African Studies Quarterly, 2000, Vol.3, No.3, pp.1-21.

Shaffer, G., 'Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements', Columbia Journal of European Law, 2002, Vol.9, No.1, pp.29-78.

Shalini, R.T., 'Are Mauritians ready for e-Government Services?,' Government Information Quarterly, 2009, Vol.26, No.3, pp.536-539.

Shih, C., 'Opening the Dichotomy of Universalism and Relativism' A Review of Negotiating Culture and Human Rights edited by Linda S. Bell, Andrew J. Nathan and Ilan Peleg. New York: Columbia University Press, 2001.

Shivji, I.G., The Concept of Human Rights in Africa, Dakar, Codesria, 1989.

Shoemaker, D.W., 'Self-Exposure and Exposure of the Self: Informational Privacy and the Presentation of Identity', Ethics and Information Technology, 2010, Vol.12, No.1, pp.3-15.

Siems, M.M., 'The Taxonomy of Interdisciplinary Legal Research: Finding the Way out of the Desert', Journal of Commonwealth Law and Legal Education, 2009, Vol.7, No.1, pp.5-17.

Sihlongonyane, M.F., 'The Invisible Hand of the Family in the Underdevelopment of Africa Societies: An African Perspective', Scholarly Paper Series 1.

Sindima, H., 'Liberalism and African Culture', Journal of Black Studies, 1990, Vol.21, No.2, pp.190-209.

Sinjela, M., 'Constitutionalism in Africa: Emerging Trends', The Review, Special Issue, 1998, Vol.23, No.60, pp.23-29.

Solove, D.J, 'Conceptualising Privacy', California Law Review, 2002, Vol. 90, No. 4, pp. 1087-1156.

Solove, D.J., 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', Stanford Law Review, 2001, Vol. 53, No.6, pp. 1393-1462.

Solove, D.J., "I've Got Nothing to Hide" and Other Misunderstandings of Privacy', San Diego Law Review, 2007, Vol.44, No.4, pp.745-772.

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

Somek, A., 'Postconstitutional Treaty', German Law Journal, 2007, Vol.8, No. 12, pp.1121-1132.

Stewart, B., 'A Comparative Survey of Data Protection Authorities-Part1: Form and Structure', Privacy Law and Policy Reporter, 2004, Vol.11, No.2, corrigan.austlii.edu.au (accessed 19/03/2012).

Stewart, B., 'A Comparative Survey of Data Protection Authorities-Part2: Independence and Functions', Privacy Law and Policy Reporter, 2004, Vol.11, No.3, corrigan.austlii.edu.au (accessed 19/03/2012).

Stewart, B., 'Proposed Amendments to NZ Privacy Act give "Adequate Protection"', Privacy Law & Policy Reporter, 2001, Vol.5, www.austlii.edu.au (accessed 1/11/2011).

Stewart, B., 'Towards Global Solutions: APEC Ministers endorse Cross-Border Privacy Rules Scheme', Privacy Laws & Business International Report, 2011, No.114, pp.14-15.

Sutherland, E., 'The Mandatory Registration of SIM Cards', Computer and Telecommunications Law Review, 2010, Vol.16, No.3, pp.61-63.

Taiwo, O., Colonialism Pre-empted Modernity in Africa, Indiana University Press, U.S.A, 2010.

Talbi, M., 'Religious Liberty as Divine Gift', ISLAMI 21 Monitor, 2010, Issue 52-53.

Tambulasi, R and Kayuni, H., 'Can African Feet Divorce Western Shoes? The Case of "Ubuntu" and Democratic Good Governance in Malawi', Nordic Journal of African Studies, 2005, Vol.14, No.2, pp.147-161.

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

Tanoh, A and Adjolohoum, H., 'International Law and Human rights litigation in Côte d'Ivoire and Benin', Killander, M(ed)., International Law and Domestic Human rights Litigation in Africa, Pretoria University Law Press(PULP), South Africa, 2010, pp.109-120.

Tanzania Institute of Education., Africa from Stone Age to the Nineteenth Century, NPC-KIUTA, Dar es Salaam, 2002.

Tavani, H.T., 'Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy', METAPHILOSOPHY, 2007, Vol.38, No.1, pp. 1-22.

Taylor, N., 'State Surveillance and the Right to Privacy', Surveillance & Society, 2002, Vol.1, No.1, pp.66-85.

The Editors of the Spark, Some Essential Features of Nkurumaism, International Publishers, New York, 1965.

The Wold Bank., Legal Aspects of HIV/AIDS: A Guide for Policy and Law Reform, The World Bank, Washington, D.C, U.S.A, 2007.

Thierer, A., 'Book Review: Solove's Understanding Privacy', The Technology Liberation Front, 2008.

Thomas, V.M and Schoeneman, T.J., 'Individualism versus Collectivism: A Comparison of Kenyan and American Self-Concepts', Basic and Applied Social Psychology, 1997, Vol.19, No.2, pp.261-273.

Thompson, J.J., 'The Right to Privacy', Philosophy and Public Affairs, 1975, Vol.4, No.4, pp.295-314.

Traca J.L and Embry, B., 'The Angolan Data Protection Act: First Impressions', International Data Privacy Law, 2011, International Data Privacy Law, 2012, Vol.2, No.1, pp.40-45.

Traca, J.L and Embry, B., 'An Overview of the Legal Regime for Data Protection in Cape Verde', International Data Privacy Law, 2011, Vol.1, No.4, pp.249-255.

Turle, M., 'Durant v FSA-Court of appeal's Radical Judgment on the Data Protection Act', Computer Law & Security Report, 2004, Vol. 20, No.2, pp.133-136.

Turle, M., 'Freedom of Information and Data Protection-A Conflict or Reconciliation', Computer Law and Security Report, 2007, Vol. 23, pp.514-522.

Ubena, J., 'Privacy: A Forgotten Right in Tanzania', the Tanzania Lawyer, 2012, Vol.1, No.2, pp. 72-114.

Ugochukwu, B. E., 'Africanizing' Human Rights in Africa: Nigeria and Kenya Constitutions in Context', Working Paper Series, Social Science Research Network, 2010, pp.1-38.

Van der Veen, L.J, *et al.*, 'Language, Culture and Genes in Bantu: a Multidisciplinary Approach of the Bantu-Speaking Populations of Africa', OMLL-01_JA27:01-B07/01-S08/01-Vo1.

Van der Vyver, J. D., 'State-Sponsored Proselytization: A South African Experience', Emory International Law Review, 2000, Vol. 14, pp.779-848.

Van der Walt, J.C and Midgley, J.R., Principles of *Delict*, Butterworths, South Africa, 2005.

Van Rensburg. J., 'CCTV Security and Safety Security/Safety Equipment – Africa', International Market Insight. 2001, Strategis: Industry Canada.

Vogt, L and Laher, S., 'The Five Factor Model of Personality and Individualism/Collectivism in South Africa: An Exploratory Study', Psychology in Society, 2009, No.37, pp.39-54.

Volkman, R., 'Privacy as Life, Liberty, Property', Ethics and Information Technology, 2003, Vol.5, No.4, pp.199-210.

Vu, L *et al.*, 'Disclosure of HIV Status to Sex Partners Among HIV-Infected Men and Women in Cape Town, South Africa', AIDS Behav, 2012, Vol.16, No.1, pp.132-138.

Wa Thiong'o, N., The River Between, East African Educational Publishers Ltd, Nairobi/Kampala/Dar es Salaam, 2007.

Wacks, R., '"Private Facts": Is Naomi Campbell a Good Model?', SCRIPTed 2004, Vol.1, No.3,pp.420-433.

Wacks, R., Personal Information: Privacy and the Law, Oxford: Clarendon Press, 1993.

Warren, S.D and Brandeis, L.S., 'The Right to Privacy,' Harvard Law Review, 1890, Vol.4, No.5, pp.193-195.

Wasserman, H and Boloka, M., 'Privacy, the Press and the Public Interest in Post-Apartheid South Africa', Parliamentary Affairs, 2004, Vol.57, No.1, pp.185-195.

Waters, N., 'The APEC Asia-Pacific Privacy Initiative-A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation?', SCRIPTed, 2009, Vol.6, No.1, pp.74-89.

Watts, M., 'Information, Data and Personal Data-Reflections on *Durant v. Financial Services Authority*', Computer Law & Security Report, 2006, Vol. 22, No.4, pp.320-325.

Weiser, S.D *et al.*, 'Routine HIV Testing in Botswana: A Population-Based Study on Attitudes, Practices, and Human Rights Concens', PLoS Medicine, 2006, Vol.3, No.7, pp.1013-1022.

Weldon, G., 'A Comparative Study of the Construction of Memory and Identity in the Curriculum of Post-Conflict Societies: Rwanda and South Africa', International Journal of Historical Learning, Teaching and Research, 2003, Vol.3, No.2, pp.55-72.

Welsh, D., The Rise and Fall of Apartheid, Jonathan Ball Publishers, Johannesburg/Cape Town, 2009.

Westin, A., 'Privacy in America: An Historical and Socio-Political Analysis', National Privacy and Public Policy Symposium, Hartford, 1995.

Westin, A.F, Privacy and Freedom, Atheneum Press, New York, 1967.

Whitaker, R., The End of Privacy: How Total Surveillance Is Becoming a Reality, The New Press, New York, 1999.

Whitley, E.A., 'Informational Privacy, Consent and the "Control" of Personal Data', Information Security Technical Report, 2009, Vol.14, No.3, pp.154-159.

Williams, G., Learning the Law, 11th Edition, Universal Law Publishing Co. Pvt. Ltd under special arrangement with Sweet & Maxwell, New Delhi, 2002.

Wilson, G., 'Comparative Legal Scholarship' in W.H Chui, and M. McConville, (eds), Research Methods for Law, Edinburgh University Press, 2010, pp. 87-103.

Wing, A.K., 'Communitarianism vs. Individualism: Constitutionalism in Namibia and South Africa', Wisconsin International Law Journal, 1992-1993, Vol.11, No.2, pp.295-380.

Xu, H *et al*., 'Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View', International Conference on Information Systems (ICIS) Proceedings, 2008, pp.1-16.

Yao-Huai, L., 'Privacy and Data Privacy Issues in Contemporary China', Ethics and Information Technology, 2005, Vol.7, pp.7-15.

Zimmerman, R.K., 'The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century', Journal of Legislation and Public Policy, 2000, Vol. 4, pp. 439-464.

Zoller, E., 'The Treaty Establishing a Constitution for Europe and the Democratic Legitimacy of the European Union', Indiana Journal of Global Legal Studies, 2005, Vol.12, No.2, pp.390-408.

B. Dissertations/Theses, Paper Presentations and Surveys

Akinsuyi, F.F., 'Data Protection Legislation for Nigeria, The Time is Now!', Nigerian Muse, www.nigerianmuse.com (accessed 11/10/2011).

Anspach, P., 'The Indigenous Rights of Personality with Particular Reference to the Swazi in the Kingdom of Swaziland', PhD thesis, University of South Africa, 2004.

Archick, K and Mix, D.E., 'The European Union's Reform Process: The Lisbon Treaty', Congressional Research Service (CRS) Report for Congress, 2009, pp.1-9.

Archick, K., 'The European Union's Constitution', Congressional Research Service (CRS) Report for Congress, 2005, pp.1-6.

Bakari, J.K., 'A Holistic Approach for Managing ICT Security in Non-Commercial Organisations: A Case Study in a Developing Country', Doctoral Dissertation, University of Stockholm, Sweden, 2007.

Bakibinga, E. M., 'Managing Electronic Privacy in the Telecommunications Sub-Sector: The Ugandan Perspective', 2004, thepublicvoic.org, (accessed 3/10/2011).

Baruh, L., 'The Guilty Pleasure of Watching like Big Brother: Privacy Attitudes, Voyeurism and Reality Programs', January, 2007, a dissertation available from ProQuest, www.repository.upenn.edu, (accessed 3/10/2011).

Bennett, C.J and Raab, C.D., 'The Governance of Global Issues: Protecting Privacy in Personal Information', A Paper presented in the European Consortium for Political Research, March 28- April 2, 2003.

Bennett, C.J., 'International Privacy Standards: A Continuing Convergence' www.colinbennett.ca, (accessed 11/10/2011).

Chenwi, L.M., 'National Human Rights Institutions: A Comparative Study of the National Commissions on Human Rights of Cameroon and South Africa', LL.M Thesis, University of Pretoria, South Africa, 2002.

Dossow, R., 'The Interception of Communications and Unauthorised Access to Information stored on Computer Systems in the Light of the European Convention on Human Rights', pp.1-8, www.europarl.europa.eu (accessed 14/12/2011).

Enyew, A.B., 'Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia', LL.M Thesis, University of Oslo, Norway, 2009.

Ferraro, G., 'Rural and Urban Population in Swaziland: Some Sociological Considerations', National Symposium on Population and Development, 26-29 May 1980, Mbabane, Swaziland.

FitzGerald, J.R.S., 'The Last of the Maasai in Northern Tanzania?-Redefining Cultural Identity', M.A Thesis, Oxford Brookes University, 2008.

Gade, C.B.N., '*Ubuntu* and the South African Truth and Reconciliation Process', M.A Thesis, Aarhus University, Denmark, 2010.

Gentili, A.M., 'Party, Party Systems and Democratisation in Sub-Saharan Africa', Paper Presentation at the Sixth Global Forum on Reinventing Government, Seoul, Republic of Korea, 24-27 May 2005, unpan1.un.org, (accessed 4/02/2012).

Girvan, N., 'The Post Colonial Economy and Society: Facing the Challenge', Paper prepared for presentation at the Regional Forum of Projects Promotion Ltd., St Vincent and the Grenadines, February 11, 2008, pp.1-16.

Gorska, Z.M., 'Privacy, Surveillance and HIV/Aids in the Workplace: A South African Case Study', M.A Thesis, University of Witwatersrand, Johannesburg, 2008.

Guðmundsdóttir, G.B., 'Approaching the Digital Divide in South Africa', NETREED Conference, 5-7, December, 2005, Beitostølen, Norway.

Hubbard, A., 'Does the Safe Harbor Agreement have a future? If so, what kind?', A Tutorial Paper presented at the Norwegian Research Centre for Computers and Law (NRCCL), Spring, 2006, pp.1-10.

Humphreys, L *et al*., 'How much is too much? Privacy issues on Twitter' www2.research.att.com, (accessed 3/10/2011).

Hustinx, P., 'Data Protection and Cloud Computing under EU Law', Third European Cyber Security Awareness Day BSA, European Parliament, 13 April 2010, pp.1-7.

Izuogu, C.E., 'Nigeria: Data Protection & Privacy Issues in NCC's Directive on SIM Card Registration', 2010, www.facebook.com, (accessed 11/10/2011).

Karanja, S.K., 'Schengen Information System and Border Control Co-Operation: A Transparency and Proportionality Evaluation', PhD Thesis, Faculty of Law, University of Oslo, 2006.

Ladan, M.T., 'The Role of Law in the HIV/AIDS Policy:-Trend of Case Law in Nigeria and Other Jurisdictions', Inaugural Lecture delivered at the Ahmadu Bello University, Zaria, Nigeria, 2008, pp.1-64.

Loukidelis, D., 'Transborder Data Flows & Privacy-An Update on Work in Progress', Paper Presentation at the 7th Annual Privacy & Security Conference, Victoria, BC, February 10, 2006, pp.1-17.

Madhub, D., 'A Legal Purview of the Data Protection Act and the Mission of the Data Protection Office' presented to Mauritius Employers Federation members, Port Louis, 26 January 2010.

Madhub, D., 'An overview of the Data Protection Act and its implications as regards registration transfers of personal data and data subject access requests' for the banking sector' presented to the Mauritius Bankers' Association, Port Louis, 5 June 2009.

Madhub, D., 'An overview of the Data Protection Act and its implications as regards registration and data subject access requests for the Ministry of Information and Communication Technology' presented to the Ministry of Information and Communication Technology, Port Louis, 10 June 2009.

Madhub, D., 'An Overview of the Mauritian Data Protection Act' presented on the occasion of the Cyber Security Conference, Port Louis, 30 November 2007.

Madhub, D., 'Analysis of the Obligations of a Data Controller and a Data Processor' presented to Data Protection Compliance Officers organised by Geroudis Management Services Ltd Port Louis, 11 November 2010.

Madhub, D., 'Data protection from an employment perspective' presented to Groupe Mon Loisir Ltd, Port Louis, 5 July 2011.

Madhub, D., 'Data Protection Fundamentals for the Banking Sector' presented to Barclays Bank, Port Louis, 26 April 2012.

Madhub, D., 'Data Protection Implications for the Public Sector' presented to the Ministerial Security Committee in collaboration with the National Security Advisor's Office, Port Louis, 16 September 2009.

Madhub, D., 'Data Protection Requirements for the ITES/BPO/KPO/LPO sector' presented at MEF-MCCI Building, Ebene in collaboration with OTAM, Port Louis, 03 September 2009.

Madhub, D., 'Ensuring compliance with data protection principles from a practical perspective' presented on the occasion of the Computer Security Day 2009, Port Louis, 30 November 2009.

Madhub, D., 'How to Ensure Effective Compliance with the Data Protection Act' presented to Lamco Insurance Ltd, Port Louis, 18 January 2011.

Madhub, D., 'How to incorporate data protection rules to safeguard shareholders' personal data of the sugar investment trust' presented to the representative of SIT, Port Louis, 25 March 2011.

Madhub, D., 'La problématique juridictionnelle et les enjeux du transfert de données personnelles dans les opérations d'externalisation' presented to AFAPDP, Dakar, 21 September 2011.

Madhub, D., 'Les Propositions apportées par la commissaire au projet de loi mauricien visant à protéger les enfants à l' ère numérique' presented to the Francophone Conference, Madrid, 2 November 2009.

Madhub, D., 'Making Sense of it:- What is Data Protection?' presented to the Truth and Justice Commission, Port Louis, 09 March 2011.

Madhub, D., 'Overview of the Fundamental Aspects of the Right of Access' presented to Mutual Aid Association Staff, Port Louis, 20 April 2012.

Madhub, D., 'Overview of the Fundamental Aspects of the Right to Access' presented to Mutual Aid Association Staff, Port Louis, 20 April 2012.

Madhub, D., 'Overview of the legal requirements imposed by the Data Protection Act on data controllers and the corresponding rights of data subjects' presented to students at the University of Technology, Port Louis, 10 March 2009.

Madhub, D., 'The Data Protection Act - An introduction to its implications and objectives' presented to the staff of the Local Government Service Commission, Port Louis, 13 August 2010.

Madhub, D., 'The Data Protection Implications for our DNA Bill' presented at the Awareness Workshop on Legal Aspects of the Use of Human DNA, Port Louis, 9 June 2009.

Madhub, D., 'The Data Protection Obligations of a Public Institution' presented to the Ministry of Social Security at the Training Unit of the Ministry, Port Louis, 5 October 2010.

Madhub, D., 'The Data Protection Office in Mauritius - The Challenges Ahead' presented to ICT-BPO Forum, Port Louis, 5 October 2011.

Madhub, D., 'The Obligations of a Public Data Controller and Processor under the Data Protection Act' presented to the Ministry of Health, Port Louis, 16 November 2010.

Madhub, D., 'Video on Data Protection' presented to International Card Processing Ltd and others, Port Louis, 12 August 2011.

Madhub, D.,'A simplified understanding of the intricacies of the Data Protection Act and how the implementation of this legislation will affect your daily life' presented for workshop on Privacy and Data Protection organised in collaboration with the National Computer Board, Port Louis, 27 February 2009.

Madhub, D.,'The challenges imposed by biometric technology on data protection and privacy' presented on the occasion of the Computer Security Day 2008, Port Louis, 1 December 2008.

Maggio, N., ""The Whole Earth as Village": A Chronotopic Analysis of Marshall McLuhan's 'Global Village' and Patrick McGoohan's The Prisoner' M.A Thesis, Brock University, Ontario, 2008.

Makulilo, A.B., 'Does the Lindqvist Decision by the ECJ make sense in terms of its treatment of the application of Art 25 of Directive 95/46/EC to uploading and downloading of personal information on internet homepages?' A Tutorial Paper presented at the Norwegian Research Centre for Computers and Law (NRCCL), Spring, 2006.

Makulilo, A.B., 'State-Party and Democracy: Tanzania and Zambia in Comparative Perspective', PhD Thesis, University of Leipzig, 2010.

Makulilo, A.B., 'The Admissibility of Computer Printouts in Tanzania: Should it be any Different Than Traditional Paper Document?', LL.M Thesis, University of Oslo(Norway), 2006.

Marchini, R., 'United Kingdom Changes in Case Law Update, Part 1: Reconciling the Irreconcilable-the *Harcup* Information Tribunal Decision pits *Durant* against ICO Guidance', World Data Protection Report, March, 2008.

Mayer, J., 'Globalisation, Technology Transfer and Skill Accumulation in Low-Income Countries', United Nations Conference on Trade and Development, Geneva, August, 2000.

Messele, R., 'Enforcement of Human Rights in Ethiopia', Research Subcontracted by Action Professionals' Association for the People(APA), 31st August 2002.

Michael, A., 'The Decision and Implementation of Privatization in Tanzania', M.A Thesis, Institute of Social Studies, The Netherlands, 2002.

Mireku, O., 'Three Most Important Features of South African Legal System that Others Should Understand', IALS Conference, www.ialsnet.org, (accessed 7/04/2012).

Mivule, K and Turner, C., 'Applying Data Privacy Techniques on Tabular Data in Uganda', arxiv.org, (accessed 4/10/2011).

Munir, A.B., 'Implementation of the APEC Privacy Framework in National Regulation', Paper Presentation during Workshop on International Data Sharing and Biometric Identification, Royal Plaza Hotel, Singapore, 2-3 July 2009.

Ndayikengurukiye, M., 'The International Human Rights Law as a source of Law in the Burundian Judicial System', LL.M Dissertation, University of Makerere, Uganda, 2005.

Neethling, J., *'Die Reg op Privaatheid'*, LL.D Thesis, UNISA, 1976.

Neuwirt, K., 'Acceso a la información y protección de datos personales: dos caras de un mismo derecho-2 Seminario Internationacional, Connvention 108: New Challenges for Data Protection in Non-European States', 13-14 November 2008, Mexico City.

Nwanko, I.S., 'Part I: Nigeria's SIM Card Registration Regulations 2010: The Implications of unguarded Personal Data Collection', www.facebook.com (accessed 11/10/2011).

Nwanko, I.S., 'Part II: Nigeria's SIM Card Registration Regulations 2010: The Implications of unguarded Personal Data Collection', www.facebook.com (accessed 11/10/2011).

Ozoemana, R.N., 'African Customary Law and Gender Justice in a Progressive Democracy', LL.M Thesis, Rhodes University, 2006.

Plückhahn, P., '(E-Commerce) Data Protection in the European Union and South Africa: A Comparative Study', Msc Thesis, Aarhus University (Denmark), 2010.

Polakiewicz, J., 'Convention 108 as a Global Privacy Standard?' International Data Protection Conference, Budapest, 17 June 2011.

Raab, C.D., 'Roles and Relationships of Data Protection Authorities', Presentation at the Conference on 'The Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information 1995 – 2011' Budapest, 28 September 2011, pp. 1-24.

Razak, A.A., 'Understanding Legal Research', Department of Management and Marketing Faculty of Economics and Management, University Putra Malaysia, econ.upm.edu.my (accessed 25/09/2011).

Reding, V., 'The Future of Data Protection and Transatlantic Cooperation', Speech at the 2nd Annual European Data Protection and Privacy Conference (SPEECH/11/851), Brussels, 6 December 2011, pp. 1-4, at p.4.

Richner, J.E., 'The Historiographical Development of the Concept "mfecane" and the Writing of Early Southern African History, from 1820s to 1920s', M.A Thesis, Rhodes University, 2005.

Ringou, N., 'Data Protection: European Adequacy Procedure', presentation made in 'Twinning Project IS/2007/ENPAP/JH/01: Strengthening Data Protection in Israel' 30 September 2009, Israel, (23 slides, at slide no.17),www.justice.gov.il(accessed 11/01/2012).

Room, S., 'Does *Lindqvist* reveal a Need for a *De Minimis* Principle in Directive 95/46/EC?', LL.M Thesis, Queen Mary University of London, 2004.

Roos, A., 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study', LL.D Thesis, UNISA, 2003.

Slemrod, J., 'Taxation and Big Brother: Information, Personalisation, and Privacy in 21st Century Tax Policy', a lecture given at the Annual Lecture to the Institute of Fiscal Studies, London, September, 26, 2005.

Tadesse, M.A., 'HIV Testing from an African Human Rights System Perspective: An Analysis of the Legal and Policy Framework of Botswana, Ethiopia and Uganda', LL.M Thesis, University of Pretoria, South Africa, 2007.

Tan, J.G., 'What effect is the APEC Privacy Framework likely to have in the struggle between the EU and APEC states to establish global standards for data protection?', A Tutorial Paper presented at the Norwegian Research Centre for Computers and Law (NRCCL), Spring, 2006, pp.1-9.

Taylor, K., 'Awareness Survey on Freedom of Information and Data Protection Legislation and Open Government Data Initiatives', The Internet Governance Forum, Nairobi, Kenya, 27th -30th September 2011, pp.1-19.

The Working Group-Latin America Data Protection Network, 'Self-Regulation and Personal Data Protection', Conference at Santa Cruz De La Sierra-Bolivia, 3-5 May 2006, pp.1-13.

Toops, E.E., 'Why is there No EU Constitution? An Analysis of Institutional Constitution-Making in the European Union', B.A Thesis, University of Pennsylvania, 2010.

Ulyashyna, L., 'Does case law developed by the European Court of human Rights pursuant to ECHR Article 8 add anything substantial to the rules and principles found in ordinary data protection principle?', A Tutorial Paper presented at the Norwegian Centre for Computers and Law(NRCCL), Spring, 2006.

Walden, I., 'East African Community Task Force on Cyber Laws: Comparative Review and Draft Legal Framework', Draft v.1.0, 2/5/08 prepared on behalf of UNCTAD and the EAC, May 2008.

Watson, C. A., 'Internet Research Methodology', 2004 Presentations, Paper 8, p.7, digitalcommons.law.uga.edu (accessed 26/09/2011).

Wiley, J., 'The Globalisation of Technology to Developing Countries', Global Studies Student Papers, Paper No.3, digitalcommons.providence.edu (accessed 3/10/2011).

C. Reports and Other Documents

EAST AFRICAN COMMUNITY

EAC, Background Paper for the Second Meeting of the EAC Task Force on Cyberlaws, Golf Course Hotel, Kampala, Uganda, 23rd -25th June 2008, EAC/TF/2/2008, (Annex I).

EAC, Report of the 2nd EAC Regional Task Force Meeting on Cyberlaws, Golf Course Hotel, Kampala, Uganda, 23rd -25th June 2008, EAC/TF/2/2008.

EAC, Draft EAC Legal Framework for Cyber Laws, (Phase I) November 2008.

Legal Notice No. EAC/8/2007, East African Community Gazette, Vol.AT 1-No.0004, Arusha 30th December 2007.

UNCTAD, Press Clipping: EAC Develops Cyber Laws, 25/10/2011.

EUROPEAN UNION

Article 29 Working Party

Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy, XV D/5020/97/ EN, WP 4, (adopted on 26th June 1997).

Opinion 01/2o12 on the Data Protection Reform Proposals, 00530/12/EN, WP 191(adopted on 23rd March 2012).

Opinion 1/2004 on the Level of Protection of Personal Data ensured in Australia for the Transmission of Passenger Name Record Data from Airlines, 10031/03/EN, WP 85, (adopted on 16th January 2004).

Opinion 1/2005 on the Level of Protection ensured in Canada for the Transmission of Passenger Name Record and Advance Passenger Information from Airlines, 1112/05/EN, WP 103, (adopted on 19th January 2005).

Opinion 1/2008 on Data protection Issues related to Search Engines, 00737/EN, WP 148, (adopted on 4th April 2008).

Opinion 1/2010 on the concepts "Controller" and "Processor", 00264/10/EN, WP164, (adopted on 16th February 2010).

Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, 5092/98/EN/final, WP 15, (adopted on 26th January 1999).

Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand, 00665/11/EN, WP182, (adopted on 4th April 2011).

Opinion 15/2011 on the Definition of Consent, 01197/11/EN, WP187, p.8, (adopted 13th July 2011).

Opinion 2/99 on the Adequacy of the 'International Safe Harbor Principles' issued by the U.S Department of Commerce on 19th April 1999, 5047/99/EN/final, WP 19, (adopted on 3rd May 1999).

Opinion 3/2000 on the EU/U.S dialogue concerning the 'Safe Harbor' arrangement, 5019/00/EN/FINAL, WP 31, (adopted on 16th March 2000).

Opinion 3/2001 on the Adequacy Level of the Canadian Personal Information and Electronic Documents Act, 5109/00/EN, WP 39, (adopted on 26th January 2001).

Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000, 5095/00/EN, WP 40.

Opinion 3/2004 on the Level of Protection ensured in Canada for the Transmission of Passenger Name Records and Advance Passenger Information from Airlines, 10037/04/EN, WP 88, (adopted on 11th February 2004).

Opinion 4/2000 on the level of protection provided by 'Safe Harbor Principles', CA07/434/00/EN, WP 32, (adopted on 16th May 2000).

Opinion 4/2002 on the Level of Protection of Personal Data in Argentina, 11081/02/EN, WP 63, (adopted on 3rd October 2002).

Opinion 4/2007 on the concept of Personal Data, 01248/07/EN, WP136, (adopted on 20th June 2007).

Opinion 4/99 on the Frequently Asked Questions to be issued by the U.S Department of Commerce in relation to the proposed 'Safe Harbor Principles, 5066/99/EN/final, WP 21, (adopted on 7th June 1999).

Opinion 5/2003 on the Level of Protection of Personal Data in Guernsey, 10595/03/EN, WP 79, (adopted on 13th October 2003).

Opinion 5/2006 on the Ruling by the European Court of Justice of 30 May 2006 in Joined cases C-317/04 and C-318/04 on the Transmission of Passenger Name Records to the United States, 1015/06/EN, WP 122, (adopted on 14th June 2006).

Opinion 5/2007 on the Follow-up Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record(PNR) Data by Air Carriers to the United States Department of Homeland Security concluded in July 2007, 01646/07/EN, WP 138, (adopted on 17th August 2007).

Opinion 5/2009 on Online Social Networking, 01189/09/EN, WP 163, (adopted on 12th June 2009).

Opinion 5/99 on the Level of Protection of Personal Data in Switzerland, 5054/99, WP 22, (adopted on 7th June 1999).

Opinion 6/2002 on Transmission of Passenger Manifest Information and other Data from Airlines to the United States, 11647/02/EN, WP 66, (adopted on 24th October 2002).

Opinion 6/2003 on the Level of Protection of Personal Data in the Isle of Man, 11580/03/EN, WP 82, (adopted on 21st November 2003).

Opinion 6/2009 on the Level of Protection of Personal Data in Israel, 02316/09/EN, WP 165, (adopted on 1st December 2009).

Opinion 6/2010 on the Level of Protection of Personal Data in the Eastern Republic of Uruguay, 0475/10/EN, WP 177, (adopted on 12th October 2010).

Opinion 6/99 on the Level of Personal Data Protection in Hungary, 5070/EN/99, WP 24, (adopted on 7th September 1999).

Opinion 7/2006 on the Ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the Transmission of Passenger Name Records to the United States and the urgent Need for a new Agreement, 1612/06/EN, WP 124, (adopted on 27th September 2006).

Opinion 7/2007 on the Level of Protection of Personal Data in the Principality of Andorra, 02317/09/EN, WP 166, (adopted on 1st December 2009).

Opinion 7/99 on the Level of Data Protection provided by the 'Safe Harbor' Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the U.S Department of Commerce, 5146/99/EN/final, WP 27, (adopted on 3rd December 1999).

Opinion 8/2004 on the Information for Passengers concerning the Transfer of PNR Data on Flights between the European Union and the United States of America, 11733/04/EN, WP 97, (adopted on 30th September 2004).

Opinion 8/2007 on the Level of Protection of Personal Data in Jersey, 02072/07EN, WP 141, (adopted on 9th October 2007).

Opinion 9/2007 on the Level of Protection of Personal Data in the Faroe Islands, 02107/07/EN, WP 142, (adopted on 9th October 2007).

Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU based Websites, 5035/01/EN/Final, WP 56, (adopted on 30th May 2002), pp.10-12.

Working Document on Functioning of the Safe Harbor Agreement, 11194/02/EN, WP 62, (adopted on 2nd July 2002).

Working Document on Privacy on the Internet: An Intergraded EU Approach to Online Data Protection, 5063/00/EN/FINAL, WP 37, (adopted on 21st November 2000).

Working Document on processing of personal data on the Internet, 5013/99/EN/final, WP 16, (adopted on 23rd February 1999).

Working Document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning 'the International Safe Harbor Principles, 5075/99/EN/final, WP 23, (adopted on 7th July 1999).

Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, DG XV D/5025/98/WP 12, (adopted on 24th July 1998).

European Commission

'Personal data-more use, more Protection?' Press Release from the Commission inviting stakeholders to register and attend the Data Protection Conference, 19-20 May 2009, in Brussels, Belgium.

A Comprehensive Approach on Personal Data Protection in the European Union, COM (2010)609 final, Brussels, 4 November 2010, pp.1-19.

Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data', COM (92) 422 final, 15 October 1992.

Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer 359, November-December 2010.

COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, C(2003) 1731 of 30 June 2003 – O.J.L 168, 5/7/2003.

COMMISSION DECISION on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, C(2004) 1914 of 14 May 2004.

COMMISSION DECISION on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, C(2005) 3248 of 6 September 2005.

COMMISSION DECISION on the adequate protection of personal data in Guernsey, C(2003) 4309 of 21 November 2003 – O.J.L 308, 25/11/2003.

COMMISSION DECISION on the adequate protection of personal data in the Isle of Man, C(2004) 1556 of 28 April 2004-O.J. L 151/48, 30/4/2004.

COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, 2000/518/EC of 26 July 2000 - O. J. L 215/1, 25/8/2000.

COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, C(2000) 2441 of 26 July 2000- O. J. L 215/7, 25/8/2000.

COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, C(2001) 4539 of 20 December 2001- O.J. L 2/13, 4/1/2002.

COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, C(2008) 1746 of 8 May 2008 - OJ L 138/21, 28/5/2008.

COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data, C(2010) 1130) of 5 March 2010 – O.J.L58/17, 9/3/2010.

COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra, C(2010) 7084 of 19 October 2010 – O.J. L 277/27, 21/10/2010.

COMMISSION DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, C(2011) 332 of 31 January 2011- O.J.L 27/39, 1/2/2011.

Commission Staff Working Document on the Implementation of Commission Decision 520/2000/EC on the adequacy protection of personal data provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the U.S Department of Commerce, SEC82004) 1323, Brussels, 20.10.2004.

COUNCIL DECISION on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data, 2006/230/EC of 18 June 2005-O.J.L 82/14, 21/3/2006.

CRID., Analysis of the adequacy of protection of personal data provided in Mauritius: draft final report, 2010.

CRID., First analysis of the personal data protection law in Israel in order to determinate whether a second step has to be undertaken (confidentiel), 2006.

CRID., First analysis of the personal data protection law in Japan in order to determinate whether a second step has to be undertaken (confidentiel), 2006.

CRID., First analysis of the personal data protection law in Kosovo in order to determinate whether a second step has to be undertaken : final report (confidentiel), 2006.

CRID., First analysis of the personal datat protection in Montenegro to determinate whether a second step has to be undertaken : final report (confidentiel), 2006.

CRID., First analysis of the personal data protection in Serbia to determinate whether a second step has to be undertaken : final report (confidential), 2006.

CRID., Analysis of the adequacy of protection of personal data in the Faeroe Islands (confidential), 2006.

CRID., Analysis of the Adequacy of Protection of Personal Data provided in Tunisia-Final Report, 2010.

CRID., First analysis of the personal data protection law in Bosnia and Herzegovina in order to determinate whether a second step has to be undertaken (confidential), 2006.

CRID., First analysis of the personal data protection law in Fyrom in order to determinate whether a second step has to be undertaken (confidential), 2006.

CRID., First analysis on the personal data protection law in Albania to determinate whether a second step has to be undertaken : final report (confidential), 2006.

Data Protection Reforms-Frequently Asked Questions, MEMO/10/542, Brussels, November, 4, 2010, europa.eu/rapid/press Releases Action. do? Reference= MEMO/10/542.

European Commission DG Justice, Freedom and Security., 'Comparative Study on Different Approaches to New Privacy Challenges, in particular in the light of Technological Developments', Contract Nr: JLS/2008/C4/011-30-CE-0219363/00-28; Final Report, 20 January 2010.

Joint Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record(PNR) for Law Enforcement Purposes, presented by the commission on 6 November 2007, 02422/07/EN, Art 29 WP ref: WP 145, WPPJ ref: 01/07, (adopted on 5th December 2007).

Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990), final-SYN 287, 13 September 1990, pp. 21-22.

Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data, Brussels, 4 November 2010, pp.1-22.

European Council

COUNCIL DECISION 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), O.J.L204/16 of 4.08.2007.

COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service, C 2008/651/CFSP/JHA of 30 June 2008, O.J.L213/47, 08/08/2008.

MAURITIUS

Codes of Practice and Guidelines

A Practical Guide for Data Controllers & Data Processors -Volume 1

Code of Practice issued by the Data Protection Commissioner for CCTV Systems operated by the Mauritius Police Force

Data Protection-Your Rights -Volume 3

Guidelines for Handling Privacy Breaches-Volume 4

Guidelines on Privacy Impact Assessments-Volume 6

Guidelines to regulate the Processing of Personal Data by Video Surveillance Systems-Volume 5

Practical Notes on Data Sharing Good Practices for the Public and Private Sector-Volume 9

Registration Classification & Guidance Notes for Application of Data Controllers & Data Processors-Volume 2

Parliamentary Records

Mauritius National Assembly, Debate No. 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004).

Mauritius National Assembly, Debate No. 5 of 2004, 'B/165 Telephone Tapping', Parliamentary Questions-Oral Answers, Tuesday 13th April, 2004.

Mauritius National Assembly, Debate No. 7 of 2004, 'B/229 Phones (Mobile)-SMS', Parliamentary Questions-Oral Answers, Tuesday 27th April, 2004.

Reports

First Annual Report of the Data Protection Commissioner February 2009-February 2010

Mauritius Law Reform Commission Annual Report June 2004

Mauritius Research Council, Information & Communications Technology Report, 2001

Second Annual Report of the Data Protection Commissioner January 2010-December 2010

Third Annual Report of the Data Protection Commissioner January 2010-December 2011

Miscellaneous

CIA., 'Mauritius People 2012' World FactBook and Other Sources 2012

Greene, T., 'Data Protection Accreditation for Mauritius' Port Louis, Mauritius, 24 November 2011

Mauritius Housing and Population Census 2011

Mauritius National ICT Policy 2007-2011

National ICT Strategic Plan 2011-2014

Speech of H.E Mr. Alessandro Mariani, Ambassador of the European Union in Mauritius during 'Workshop for the Mauritius Data Protection Accreditation with the European Union,' Domaine Les Pailles, 24 November 2011

Speech of Mr. Tassarajen Pillay Chedumbrum, Minister of Information and Communication Technology, on Launching of E-Register at SSS Forest-Side, Boys Dept on 9 February 2011

SOUTH AFRICA

CAJ News Agency, 'SA Intelligence Faces Phone Hacking Scandal' cajnewsagency.com (accessed 10/04/2012).

Goldstuck, A., 'I am a RICA criminal', The Big Change, 2009, thebigchange.com (accessed 9/04/2012).

IT Web Security., '2010 pressure mounts on privacy Bill', 26 November 2009.

PMG ., Protection of Personal Information Bill [B9-2009] briefing, 6 October 2009.

PMG., Protection of Personal Information Bill [B9-2009] sixth working draft: technical sub-committee deliberations.

Portfolio Committee on Justice and Constitutional Development, Background Information: Protection of Personal Information Bill [B9-2009] Deliberations 4 November 2009.

Report of the Ad Hoc Joint Committee on the Open Democracy Bill [B67-98] 24 January 2000.

South African Government Gazette No. 31782 of 8 January 2009.

South African Law Reform Commission, Privacy and Data Protection, Project 124, Discussion Paper 109, October 2005.

South African Law Reform Commission, Privacy and Data Protection, Project 124, Issue Paper 24, September 2003.

South African Law Reform Commission, Privacy and Data Protection, Project 124, Report, August 2009.

The Memorandum on the Objects of the Protection of Personal Information Bill 2009.

Tilley, A., 'Airline Security sets offside trap for World Cup', BusinessDay, 22 September 2008.

UNITED KINGDOM

House of Commons, The Freedom of Information Bill: Data Protection Issues, Bill 5 of 1999-2000, Research Paper 99/99 of 3 December 1999.

TANZANIA

Parliamentary Records

BUNGE LA TANZANIA, MAJADILIANO YA BUNGE, MKUTANO WA KUMI NA MBILI, Kikao cha Arobaini na Saba – Tarehe 18 Agosti, 2008.

Reports

TCRA., 'Report on Internet and Data Services in Tanzania: A Supply-Side Survey', September 2010.

Miscellaneous

Amnesty International, 'Tanzania must end HIV "red ribbon" stigma in schools', 16th March 2012.

BBC News, 'Tanzania anger over red ribbon labels for HIV pupils', 15th March 2012.

DAILY NEWS, 27 June 2009, 'Ze Utamu bares local Police who walk away with a vendor's table caught selling at a prohibited area'.

Government Gazette, No.19 of 7th May 2010.

KULIKONI, 24 Juni 2009, 'Utapeli wa mtandao wawaliza wengi nchini'.

Makulilo, A.B., 'CCM at 34 and the Deepening Crisis', THE CITIZEN, 4th February 2011.

Mjasiri, J., 'Consumers' rights "abused", lack of awareness to blame', DAILY NEWS, 13th March 2010.

MwanaHalisi, 9-15, Desemba 2009, 'Siri za Zitto nje'.

MWANANCHI, 20 Juni 2009, 'Mzee wa Ze Utamu anaswa'.

Sani, 11-14 Julai 2009, 'Mume wa Mtu amliza Wema'.

Tanzania AIDS Week in Review, Issue No.161, February 26-March 3, 2012.

The African, 3 December 2009, 'Current Investors plunder Our Resources'.

The ARUSHA TIMES, 7-13 November 2009, 'Tanzania: SIM-Card Registration Now Viewed As Spying Move'.

THE CITIZEN, 18 February 2012, 'Mwakyembe was not poisoned, say police'.

THE CITIZEN, 19 March 2010, 'Mobile Phone Users now top 17 million'.

THE CITIZEN, 20 February 2012, 'Mwakyembe saga raises concern over team spirit'.

THE CITIZEN, 6 September 2010, 'PCCB has eye on mobile cash transfer'.

The Guardian on Sunday, 17 October 2010, 'Revealed: Kingpin behind "hateful" text messages'.

THISDAY, 24 June 2009, 'International con artists tap into local email accounts'.

THISDAY, 9 October 2009, 'Revealed: JK's health in detail'.

UNITED NATIONS

Globalisation of R&D and Developing Countries, Proceedings of the Expert Meeting, Geneva, 24-26 January, 2005.

Miscellaneous

Amnesty International., 'Uganda: Amnesty International Concerns on the Regulation of Interception of Communications Bill, 2007', Amnesty International Publications, 2007.

Amnesty International, 'Uganda: Amnesty International Memorandum on the Regulation of Interception of Communications Act 2010', Amnesty International Publications, 2010.

Anan, K., 'What is My Beef Against SIM Card Registration in Ghana?, Independent Civil Advocacy Network, 25th January 2010, www.i-can-ghana.com(accessed 19/02/2012).

Archick, K., 'The European Union's Constitution', Congressional Research Service (CRS) Report for Congress, 2005, pp.1-6.

Arieff, A *et al*., ,The Global Economic Crisis: Impact on Sub-Saharan Africa and Global Policy Responses', CRS Report for Congress, 2010.

ARTICLE 19, 'Kenya: Draft Data Protection Bill critically limited', Statement issued on 7 November 2011.

Asmah, K., 'Let's Commit To Biometric Registration', Daily Graphic, 20th January 2012,

BBC News., 'Kenya begins contentious Census', 24th August 2009,news.bbc.co.uk(accessed 21/02/2012).

Branttie, E., 'IMANI Report: The Failing SIM Card Registration Exercise- Millions of Dollars will be lost to the State. Ghana's Telecom Regulator MUST graduate SIM deactivation Exercise!' www.africanliberty.org(accessed 22/02/2012).

Business and Gadget., '2010 Census for National Development (Ghana)', www.qiam.org(accessed 21/02/2012).

Comninos, A., 'Twitter Revolutions and Cyber Crackdowns: User-Generated Content and Social Networking in the Arab Spring and Beyond', Association for Progressive Communications (APC), June 2011, pp.1-18.

Fussel, G., '*Indangamuntu* 1994: Ten years ago in Rwanda this Identity Card cost a woman her life', Prevent Genocide International, www.preventgenocide.org (accessed 19/02/2012).

Harding, C., 'Leaving the Farm: Africa's Rapid Urbanisation', How We Made It in Africa, 12 October 2011, www.howwemadeitinafrica.com (accessed 13/02/2012).

Hassan, T., 'Nigeria: National Assembly to Install Full-Body Scanners', Daily Trust, 13th December 2011.

Huff Post World., 'Kenya Holds First Census in A Decade, Causes Outcry Over Ethnic Identity', posted on 24th August, 2009.

Human Right Watch, 'The Internet in Mideast and North Africa: Free Expression and Censorship', 1999.

Human Rights Watch., 'World Report 2012: Zimbabwe Events of 2011', 2012.

IT Law Group., 'Neither a Floor nor a Ceiling: the APEC Privacy Framework fails to harmonize the Privacy Regime in the Asia Pacific Region.

Layton, R., 'When and How Can Domestic Judges and Lawyers use International Law in Dualist Systems', training.itcilo.org (accessed 28/02/2012).

Ministère de l'Economie et des Finances, Dé loc a l i s a t ion de s a c t i v i t é s de s e r v i c e s au Ma roc, Et a t de s l i eux e t oppor tuni t é s Juillet 2008.

Murungi, M., 'Registration of Mobile Phone Users: Easier said but carefully done', Kenya Law, 26th July 2009 kenyalaw.blogspot.com (accessed 19/02/2012).

Nabudere, D.W., 'Ubuntu Philosophy: Memory and Reconciliation', 2008, pp.1-20,

Nwezeh, K and Eze, C., 'Nigeria: Abdulmutallab-Ministers, Foreigners to Undergo Full-Body Scan', This Day, 27th January, 2010, allafrica.com(accessed 20/02/2012).

PA., 'Senior Officials to face ICC Trial over Kenya Violence', The Independent, 23rd January 2012.

Reuters Africa., 'Ethnic Question in Kenya Census stokes Suspicions', 25th August 2009,

Schmidl, M and Krone, D., 'Germany DPAs Decide EU-U.S. Safe Harbor May Not Be Relied Upon Exclusively', www.bnai.com(accessed 24/01/2012)

The Economist Intelligence Unit's Index of Democracy 2007

The Economist Intelligence Unit's Index of Democracy 2008

The Economist Intelligence Unit's Index of Democracy 2010

The Economist Intelligence Unit's Index of Democracy 2011

The Politikal Blog., 'The Great Twitter/Facebook Revolutions Fallacy', 5th February 2011,

U.S Department of State, 'Human Rights Report: Zimbabwe', 2010

UNESCO, Institute for Statistics. 'Adult and Youth Literacy', Facts Sheet, September 2011

World Bank., 'Gross National Income Per Capita 2010, Atlas Method and PPP', 2011.

Versicherung

Ich habe die Arbeit selbständig verfasst. Ich habe nur die von mir angegebenen Quellen und Hilfsmittel für die Ausarbeitung der vorgelegten Arbeit benutzt und die aus den benutzten Werken wörtlich oder inhaltlich übernommenen Stellen als solche kenntlich gemacht.

Ich habe die Grundsätze guter wissenschaftlicher Praxis bei Anfertigung der Arbeit geachtet. Insbesondere habe ich anerkannte ethische Verfahrensweisen und Grundprinzipien eingehalten, Plagzarismus jeder Art vermieden und den Grundsatz des geistigen Eigentums gewahrt.

28.05.2012 Alex Boniface Makulilo
Datum Unterschrift