DATA PROTECTION AND TRANSBORDER DATA FLOWS: IMPLICATIONS FOR NIGERIA'S INTEGRATION INTO THE GLOBAL NETWORK ECONOMY

By

ASUQUO KOFI ESSIEN ALLOTEY

Submitted in accordance with the requirements

for the degree of

DOCTOR OF LAWS

of the

UNIVERSITY OF SOUTH AFRICA

PROMOTERS: PROF A ROOS
DR G AKPAN

February 2014

Student number: **35908157**

I declare that **DATA PROTECTION AND TRANSBORDER DATA FLOWS: IMPLICATIONS FOR NIGERIA'S INTEGRATION INTO THE GLOBAL NETWORK ECONOMY** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

7th February 2014

SIGNATURE
(Mr)

DATE

ACKNOWLEDGEMENT

I am deeply grateful to God Almighty who has enabled me to complete this thesis regardless of the many challenges along the way. To Him belongs all the glory!

I could not have completed this work without the guidance of my promoters, Prof. Anneliese Roos and Dr. George Akpan. I appreciate their comments and suggestions. I thank them sincerely.

There are many others who, directly or indirectly assisted me in finishing this thesis. Some of them, in libraries in Lagos, Abuja, Alexandria and Pretoria will not see their names mentioned here, but I do acknowledge their help in getting required materials and thank them.

My family was very instrumental in getting this thesis finished; I appreciate the patience and understanding of my wife Asari, whose word processing skills was very helpful, and Beulah my daughter whose carrot cakes "sweetened" an otherwise tedious exercise. I also appreciate Naomi and Joshua, my daughter and son. I thank them all immensely for their support. I also thank my mother who did not relent in cheering me on.

A. K. Allotey, Esq.

Abuja, Nigeria

January 2014

ABBREVIATIONS

ACP	African, Caribbean and Pacific (States)
ACCI	Australian Chamber of Commerce and Industry
ACHPR	African Charter on Human and Peoples Rights
ACHPR	African Commission on Human and Peoples' Rights
ACP-EC	African, Caribbean and Pacific States – European Community
ADP	Automated Data Processing
ALRC	Australian Law Reform Commission
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Projects Agency Network
ATM	Automated Teller Machine
AU	African Union
BPE	Bureau of Public Enterprises
CHRI	Commonwealth Human Rights Initiative
CIA	Central Intelligence Agency
COE	Council of Europe
COPA	Childdren's Online Protection Act
CPNI	Customer Proprietary Network Information
CSTP	Committee for Science and Technology Policy
CUG	Computer Utilization Group
DATA	Data Accountability and Trust Act
DMA	Direct Marketing Association
DOD	Department of Defence (US)
DOJ	Department of Justice (US)
DPA	Data Protection Act/Data Protection Authorities
DPP	Director of Public Persecutions
EC	European Council/ Commission
ECHR	European Convention for the Protection of Human Rights
ECOWAS	Economic Community of West African States
EDI	Electronic Data Interchange
EEC	European Economic Community
EFCC	Economic and Financial Crimes Commission of Nigeria
EGA	European Generic Medicines Association
EIU	Economist Intelligence Unit
ENIAC	Electronic Numerical Integrator And Computer
EPIC	Electronic Privacy Information Centre
ERMA	Electronic Recording Machine Accounting
ESN	Electronic Serial Number
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCDA	Federal Capital Development Authority
FCT	Federal Capital Territory
FDI	Foreign Direct Investment
FDIC	Federal Deposit Insurance Corporation

FIPs	Fair Information Practices
FEC	Federal Executive Council
FIRS	Federal Inland Revenue Service
FOI	Freedom of Information
FSA	Financial Services Authority
FTC	Federal Trade Commission
FTP	File Transfer Protocol
FWA	Fixed Wireless Access
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDP	Gross Domestic Product
GII	Global Information Infrastructure
GLO	Global Communication (Globalcom)
GPS	Global Positioning Satellites
GSM	Global System for Mobile (Communication)
HDI	Human Development Index
HIPPA	Health Insurance Portability and Accountability Act
HTML	Hypertext Markup Language
IADIS	International Association for Development of the Information Society
IBI	Intergovernmental Bureau for Informatics
IBM	International Business Machines
IC	Integrated Circuit
ICCPR	International Convention on Civil and Political Rights
ICO	Information Commissioner's Office
ICPC	Independent Corrupt Practices and Other Related Offences Commission
ICTs	Information and Communication Technologies
IDA	Info-communications Development Authority (of Singapore)
IDRC	International Development Research Centre
IICD	International Institute for Communication and Development
IMF	International Monetary Fund
INEC	Independent National Electoral Commission
INMARSAT	International Maritime Satellite
INTELSAT	International Telecommunications Satellite
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
ITA	Information Technology Agreement
ITU	International Telecommunications Union
JAMB	Joint Admissions and Matriculation Board
JILT	Journal of Information, Law and Technology
LAN	Local Area Network
MFN	Most Favoured Nation
MIN	Mobile Identification Number

MNCs	Multinational Corporations
MRA	Media Rights Agenda
MSDOS	Microsoft Disk Operating System
MSN	Microsoft Network
NAFTA	North American Free Trade Agreement
NAFDAC	National Agency for Food and Drug Administration and Control
NBC	Nigerian Broadcasting Commission
NBTE	National Board for Technical Education
NCB	National Computer Board
NCC	Nigerian Communications Commission
NCWG	Nigerian Cybercrime Working Group
NEPA	National Electric Power Authority
NET	Nigerian External Telecommunication
NFMC	National Frequency Management Council
NGO	Non- Governmental Organisation
NIPC	Nigerian Investment Promotion Commission
NIAC	National Internet Advisory Committee
NIPOST	Nigerian Postal Service
NIST	National Institute for Standards and Technology
NITDA	National Information Technology Development Agency
NITEL	Nigerian Telecommunications Limited
NIMC	National Identity Management Commission
NPA	Nigerian Ports Authority
NPAN	Newspaper Proprietors' Association of Nigeria
NPC	National Population Commission
NPP	National Privacy Principles
NRI	Networked Readiness Index
NSA	National Security Agency
NSF	National Science Foundation
NTP	National Telecommunications Policy
NUC	National Universities Commission
NWICO	New World Information and Communications Order
OAU	Organisation of African Unity
OPC	Office of the Privacy Commissioner (Australia)
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
OPC	Oodua People's Congress/ Office of the Privacy Commissioner
OSCE	Organization for Security and Cooperation in Europe
P&T	Posts and Telecommunications
PATU	Pan African Telecommunications Union
PC	Personal Computers
PKI	Public Key Infrastructure
POS	Point Of Sale
PTO	Private Telecommunications Operator
SADC	Southern African Development Community
SALRC	South African Law Reform Commission
SAP	Structural Adjustment Programme

SIM	Subscriber Identity Module
SITA	Société Internationale des Télécommunications Aéronautiques
SMS	Short Message Service
SSL	Secure Socket Layer
TAS	Telecommunication Authority (of Singapore)
TBDF	Trans-border Data Flow
TBT	Technical Barriers to Trade
TCP	Transmission Control Protocol
TFN	Tax File Number
TGI	Transaction Generated Information
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UKAIS	UK Academy for Information Systems
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNESCO	United Nations Educational Scientific and Cultural Organisation
UNIDO	United Nations Industrial Development Organisation
UNPAN	United Nations Public Administration Network
UNRISD	United Nations Research Institute for Social Development
US	United States
USA	United States of America
USAID	United States Agency for International Development
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
USENET	User's Network
USSR	Union of Soviet Socialist Republics
VoIP	Voice over Internet Protocol
VSAT	Very Small Aperture Terminal
WAEC	West African Examinations Council
WAN	Wide Area Network
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society
WTO	World Trade Organisation
WWW	World Wide Web

SUMMARY

One of the realities that developing countries like Nigeria have to face today is that national and international markets have become more and more interconnected through the global platform of telecommunications and the Internet. This global networked economy is creating a paradigm shift in the focus of development goals and strategies particularly for developing countries. Globalisation is driving the nations of the world more into political and economic integration. These integrations are enhanced by a globally interconnected network of economic and communication systems at the apex of which is the Internet. This network of networks thrives on and encourages the expansion of cross-border flows of ideas and information, goods and services, technology and capital.

Being an active member of the global network economy is essential to Nigeria's economic development. It must plug into the network or risk being shut out. The global market network operates by means of rules and standards that are largely set by the dominant players in the network. Data protection is a critical component of the regime of rules and standards that govern the global network economy; it is evolving into an international legal order that transcends geographical boundaries.

The EU Directive on data protection is the de facto global standard for data protection; it threatens to exclude non-EU countries without an adequate level of privacy protection from the EU market. More than 50 countries have enacted data protection laws modelled on the EU standard. Access to the huge EU market is a major motivation for the current trend in global harmonisation of domestic data protection laws. This trend provides a compelling reason for examining the issues relating to data protection and trans-border data flows and their implications for Nigeria's desire to integrate into the global network economy.

There are two primary motivations for legislating restrictions on the flow of data across national boundaries. The first is the concern for the privacy of the citizens, and second, securing the economic well-being of a nation. It is important that Nigeria's privacy protection keeps pace with international norms in the provision of adequate protection for information privacy order to prevent potential impediments

to international trading opportunities.

KEY TERMS

Data protection; trans-border data flows; right to privacy in Nigeria; freedom of information; information and communication technologies; information economy; globalisation; EU Directive; OECD Guidelines, rules-based regulation.

CONTENTS

CHAPTER 1: THE RESEARCH PROBLEM 1

1. INTRODUCTION 1
1.1 The global network economy 2
1.2 The trans-border flow of information 5
1.3 Privacy and data protection after the information revolution 6
1.4 Privacy as an international trade issue 9
1.5 Getting Nigeria "connected" to the Global Network Economy 13
1.6 New norms for the digital world 15
1.7 The right to know (freedom of information) and the right to hold back information (privacy) 16

2. IDENTIFYING THE ISSUES AND THE CRITICAL QUESTIONS TO BE ANSWERED 23
2.1 Relationship between information privacy and data protection 23
2.2 Information privacy in the ICT environment 23
2.3 Data protection and Trans-border Data Flows (TBDF) 25
2.4 Critical questions to be answered 26
2.5 Assumptions 26

3. DEFINITION OF KEY TERMS 27
3.1 "Information Revolution", "Information Society", "Information Age" 27
3.2 "New Economy"/ "Information Economy" 28
3.3 Data 28
3.4 Information/personal information 29
3.5 Data protection / information privacy 29
3.6 Data processing, Trans-border Data Flow (TBDF) 30
4. RESEARCH METHOD 31
5. RESEARCH OUTLINE 32

CHAPTER 2: EMERGENCE OF THE INFORMATION ECONOMY: THE CONVERGENCE OF TECHNOLOGY, INFORMATION AND COMMERCE 37

1. INTRODUCTION: TECHNOLOGY AS CATALYST FOR HUMAN DEVELOPMENT 37
1.1 The printing press - pioneer information and communication technology 39
1.2 Newer information and communication technologies 40
1.3 Convergence of technology, information and commerce 41
1.3.1 Information society 42
1.3.2 The digital divide 44

2. THE INFORMATION ECONOMY 45
2.1 Emergence of the information economy 45
2.2 Technologies of communication and commerce 47
2.3 ICTs and international trade 48
2.4 The technologies 49
2.4.1 Introduction 49
2.4.1.1 Telegram 50
2.4.1.2 Telex 51
2.4.1.3 Telephone 51
2.4.1.4 The fax machine 52
2.4.1.5 Electronic mail 52

3. ICTs AND THE INTERNET: THEIR IMPACT ON GLOBAL COMMERCE AND TELECOMMUNICATIONS 54
3.1 Evolution of the Internet 54
3.2 Impact on global commerce 56
3.3 The Internet and developing economies 57

4. THE GLOBAL TRADE IN INFORMATION AND INFORMATION PRODUCTS 59
4.1 Introduction: Information as commodity 59
4.1.1 Information goods 60
4.1.2 Trade in services 60
4.2 Electronic commerce 62

5. GLOBALISATION, TRANS-BORDER FLOWS OF INFORMATION AND PRIVACY CONCERNS..... 64
5.1 Globalisation: economic and political perspective 64
5.2 Trans-border flows of trade-related information 67
5.3 Privacy concerns raised by TBDF 68

CHAPTER 3: THE NIGERIAN STATE AND SOCIETY IN THE INFORMATION AGE 71

1. NIGERIA: A BRIEF HISTORY OF ITS POLITICAL AND ECONOMIC DEVELOPMENT 71
1.1 Pre-1900-1969 72
1.2 1970-1999 73
1.3 1999 – present day 74
1.4 Nigeria and the information society: in or out? 78
1.4.1 The digital dilemma in Nigeria 79

2. KEY ISSUES IN NIGERIA'S COMPUTER AND INTERNET PENETRATION 84
2.1 Introduction 84
2.2 Development of information technology in Nigeria 88
2.3 Computer usage 88
2.4 Internet penetration 89
2.5 Electronic/Internet banking 91
2.6 Financial services 91

3. ACCESS TO THE INFORMATION SOCIETY IN NIGERIA 93
3.1 Telecommunications infrastructures 93
3.2 Overview of telecommunications development 93

4. REGULATORY INFRASTRUCTURE FOR TELECOMMUNICATIONS AND INTERNET USAGE... 96
4.1 Introduction 96
4.2 Institutional framework 97
4.2.1 Introduction 97
4.2.2 The Ministry of Communications Technology 97
4.2.3 The Nigerian Communications Commission 101
4.2.4 Nigerian Telecommunication Limited (NITEL) 106
4.2.5 The second national operator – Globacom Ltd 107
4.2.6 Other licenced private telecommunication operators and service providers 110
4.2.7 National Frequency Management Council (NFMC) 112

5. REGULATORY FRAMEWORK 113
5.1 Introduction 113
5.2 Regulation and competition 114
5.2.1 Objectives of the regulatory framework 114
5.2.2 Interconnection 115
5.2.3 Convergence 118
5.3 National policy on telecommunications 120
5.4 The national regulatory agencies: failure to protect information privacy 121
5.4.1 Nigerian Communications Commission (NCC) 121
5.4.1.1 The privacy implications of SIM card registration 122
5.4.2 National Information Technology Development Agency (NITDA) 127
5.5 A critical assessment of the regulatory framework 128
5.5.1 Introduction 128
5.5.2 Addressing the data protection policy problem 129

CHAPTER 4: THE LEGAL PROTECTION OF PRIVACY: A HISTORICAL, SOCIOLOGICAL AND PHILOSOPHICAL OVERVIEW 135

1. INTRODUCTION: THE RISE OF PRIVACY PROTECTION 135
1.1 What is Privacy? 138
1.1.1 The concept of privacy 138
1.1.2 Defining privacy 143
1.1.3 Information privacy 145
1.2 The rise of privacy as a legal right 145

2. HISTORICAL, SOCIOLOGICAL AND PHILOSOPHICAL ROOTS OF PRIVACY 147
2.1 Introduction 147
2.2 Western intellectual and cultural traditions 147
2.3 African/Nigerian intellectual and cultural traditions 151
2.4 Libertarianism versus communalism 153
2.5 Privacy in African/Nigerian communal cultures 154

3. RIGHT TO PRIVACY IN NIGERIA 156
3.1 Introduction 156
3.2 Statutory protection of privacy 158
3.2.1 Introduction 158
3.2.2 The relevant statutes 158
3.2.2.1 The Wireless Telegraphy Act 158
3.2.2.2 Telecommunications and Postal Offences Act 160
3.2.2.3 Statistics Act 160
3.2.2.4 NIPOST Act 161
3.2.2.5 Evidence Act 162
3.3 The Common Law connection 162
3.4 Development of English common law protection of privacy 162
3.5 Expansion of the remedy for breach of confidence 164
3.5.1 "Information must have the necessary quality of confidence about it" 166
3.5.2 "Obligation of confidence" 167
3.5.3 "Unauthorised use or disclosure of information" 168
3.5.4 The position in Nigeria today 169
3.5.5 Conclusion 177
3.6 Constitutional protection of the right to privacy 173
3.6.1 Introduction 173
3.6.2 The protection of fundamental rights 175
3.6.2.1 A brief overview of the legal system 175
3.6.2.2 Fundamental rights and the judicial process 177
3.6.2.3 The courts, the individual and the state 178
3.7 Judicial protection of the right to privacy 181
3.7.1 Introduction 181
3.7.2 Privacy protection in Nigerian case law 182
3.7.2.1 Ransome-Kuti v Att-Gen of the Federation & Ors 182
3.7.2.2 J S Olawoyin v Att-Gen. Norther Region of Nigeria 183
3.7.2.3 Cletus Madu v Neboh & Anor 184
3.7.2.4 Medical and Dental Practitioners Disciplinary Council v Dr John E N Okonkwo 186
3.8 Evaluation of privacy protection in Nigeria 188
3. 8.1 Introduction 188
3. 8.1.1 The weak notion of privacy 188
3. 8.1.2 Limited exposure to telecommunication facilities 189
3. 8.1.3 High poverty level 191
3. 8.2 Other constraints on the legal protection of privacy in Nigeria 192
3. 8.2.1 Introduction 192
3. 8.2.2 Constitutional derogations 193
3. 8.2.3 A deficient culture of respect for the rule of law 194
3. 8.3 Conclusion 196

CHAPTER 5: HOW UNREGULATED ACCESS TO INFORMATION INTERFERES WITH INFORMATION PRIVACY: RECONCILING INFORMATION PRIVACY WITH THE RIGHT TO FREEDOM OF INFORMATION 201

1 AIM OF CHAPTER 201
1.1 INTRODUCTION: ACCESS TO INFORMATION 202
1.1.1 The fundamental right to freedom of information 203
1.1.2 The individual's right to access information 204
1.1.3 Is there an obligation on government to provide information? 206
1.2 Freedom of Information laws 209
1.3. Right to freedom of information in Nigeria 211
1.3.1 Introduction: The culture of secrecy 211
1.4 The campaign for access to information in Nigeria 213
1.5 The Freedom of Information Act, 2011 215

2. UNREGULATED ACCESS TO PERSONAL INFORMATION AND THE THREATS TO INFORMATION PRIVACY 217
2.1 Introduction: Increased collection of personal information 217
2.2 The use of technology in the collection of information and record-keeping 220
2.2.1 Historical development of the use of technology for collection of information 221
2.3 The marketplace for trading personal information 224
2.3.1 New business models: their influence on the collection of personal information and threat to information privacy 225
2.3.1.1 Data brokerage industry 227
2.3.1.2 Internet search engines 229
2.3.1.3 Social networking websites 232
2.4. Other threats to the privacy of personal information 234
2.4.1 Monitoring and interception of electronic communication 235
2.4.2 Eavesdropping 237

3. BALANCING THE RIGHT TO INFORMATION AND THE RIGHT TO PRIVACY 238
3.1 The value of information privacy 238
3.2 The value of freedom of information 240
3.3 Freedom of information v information privacy in Nigeria 241
3.4 Striking the right balance between the right to information privacy and the right to freedom of information 243
3.5. Conclusion 246

CHAPTER 6: INTERNATIONAL REGULATION OF TRANS-BORDER DATA FLOWS 249

1. THE INTERNATIONAL MARKET PLACE AND TRANS-BORDER DATA FLOWS 249
1.1 Introduction 249

2 TRANS-BORDER DATA FLOWS (TBDFs) 250
2.1 Introduction: 250
2.2 Defining "trans-border data flows" 251
2.3 Emergence of the TBDF discourse 252
2.4 Major players in trans-border data flows 254
2.4. 1 Governments 254
2.4.2 Intergovernmental organisations 255
2.4.3 Multinational corporations 226
2.5 Challenges arrising from trans-border data flows 257

3. TRANS-BORDER DATA FLOWS AS THREAT TO THE PRIVACY OF PERSONAL INFORMATION 260
3.1 Introduction 260
3.2 Increased Collection of Personal Information 261
3.2.1 Data mining 262
3.2.2 Profiling 264
3.2.3 Data matching 264
3.2.4 Spam (Junk mail) 265
3.2.5 Cookies 266

4. TRANS-BORDER DATA FLOWS AS THREAT TO NATIONAL SOVEREIGNTY AND SECURITY 267
4.1 Introduction: TBDF and the transformation of sovereignty 267
4.2 The "Free Flow of Information" versus "Sovereignty over Information Flow" debate 270
4.3 Impact of TBDF and International Trade on National Sovereignty 272
4.4 National Security and Law Enforcement Concerns 274

5. LEGAL AND JURISDICTIONAL ISSUES ARISING FROM TBDFs 277
5.1 Introduction: extra-territorial Application of Domestic Laws 277
5.2 Territoriality 279
5.3 Extraterritoriality and the regulation of TBDFs..... 280
5.3.1 Jurisdiction 273

6. THE EMERGING GLOBAL DATA PROTECTION REGIME 283
6.1 Introduction: The Evolution of Trans-Border Data Flows Regulations 284
6.2 Why regulate TBDFs 284
6.3 Who controls the regulation of TBDFs? 286
6.4 An International Legal Framework for Regulation of TBDFs 288
6.5 International Harmonization of Data Protection Laws 290
6.5.1 The OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data 294
6.5.2 The Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data. 295
6.5.3 Resolution 45/95 by the General Assembly of the United Nations 296
6.5.4 UN General Assembly Draft Resolution: "The Right to Privacy in the Digital Age" 297
6.5.5 The Charter of Fundamental Rights of the European Union 298
6.5.6 ECOWAS Supplementary Act on the Protection of Personal Data within ECOWAS Region 298
6.6 The EU Directives and TBDFs 300
6.6.1 Uneven protection of information privacy across borders 300
6.6.2 The extraterritorial application of EU Directives on data protection 303
6.6.2.1 *Directive 95/46/EC* 304
6.6.2.2 *Directive 2002/58/EC (Directive on privacy and electronic communications)*..... 306
6.7 Reform of EU data protection law 312

7 SIGNIFICANCE OF THE GLOBAL DATA PROTECTION REGINE FOR NIGERIA 313

CHAPTER 7: INTEGRATING NIGERIA INTO THE GLOBAL NETWORK ECONOMY THROUGH LAW REFORM 317

1. INTRODUCTION: IMPORTANCE OF INTEGRATION INTO THE GLOBAL NETWORK ECONOMY FOR ECONOMIC DEVELOPMENT 317

2. REGULATORY STANDARDS AS BARRIER TO INTEGRATION 320
2.1 The link between trade, international standards and market access 320
2.2 Data protection legislation as barrier/gateway to the global network economy 323

3. THE EU DATA PROTECTION DIRECTIVE AS EMERGENT GLOBAL DATA PROTECTION STANDARD 326
3.1 The European Union: setting global standards 326
3.2 Is the EU Directive on privacy a violation of WTO's trade rules? 329
3.2.1 Exploring the impact of the EU *Directive* on Nigeria in relation to the WTO's trade rules.... 331
3.3 The EU process for assessing adequacy of data protection in a third country 334
3.4 Assessing the adequacy level of data protection in Nigeria 337
3.4.1 Assessing statutory and common law protection of privacy in Nigeria in the light of Directive 95/46/EC 340
3.5 Adequacy of the supervisory structure for enforcing the protection of data privacy 340
3.5.1 Evaluating the effectiveness of Nigeria's data protection system against the EU's assessment criteria 342
3.5.1.1 The "ability of the system to deliver a good level of compliance with the rules" 342
3.5.1.2 The regulatory system must be able to give sufficient "support and help to

individual data subjects in the exercise of their rights" 343
3.5.1.3 The system must be able to provide appropriate redress for the injured party where the rules are not complied with 343
3.6 Conclusions drawn from the assessment of the adequacy of data protection in Nigeria 344

4. DEVELOPING A NIGERIAN DATA PROTECTION FRAMEWORK 345
4.1 Law reform as vehicle for sustainable economic and social development 345
4.2 Establishing a regulatory framework for the digital marketplace 347
4.3 Why Nigeria should have a data protection law 349
4.3.1 To regulate the collection, processing, storage and use of personal information 349
4.3.2 To fulfil Nigeria's bilateral and multilateral treaty/convention obligations 350
4.3.3 To avoid EU sanction against data transfers to Nigeria 352
4.3.4 To provide an effective regulatory and enforcement regime for the Protection of information privacy in Nigeria 352
4.3.5 To assure international trade partners of adequate data protection 353
4.4 The newly proposed data protection law for Nigeria 355

CHAPTER 8: ENACTING A DATA PROTECTION LAW FOR NIGERIA 359
1. INTRODUCTION: MOTIVATIONS FOR ENACTING DATA PROTECTION LAWS 359
2. EXAMINING WHAT ROLE CULTURE AND ECONOMICS WILL PLAY IN SECURING THE ENACTMENT OF DATA PROTECTION LAW IN NIGERIA 360
2.1 The role of culture in the enactment of data protection legislation in Nigeria 363
2.2 The role of economic and commercial considerations in the adoption of data protection legislation in Nigeria 365
2.3 Objectives of a data protection regulatory framework 367

3. FOREIGN DATA PROTECTION LAWS AS MODELS FOR NIGERIA 368
3.1 Regulatory convergence 368
3.2 Information/data protection in other countries: A brief overview 370
3.2.1 Information privacy protection in the US 370
3.2.1.1 Enforcement of information privacy protection in US 372
3.3 Data Protection in the UK 373
3.3.1 Data Protection Act 1998 373
3.3.1.1 Regulatory and enforcement institutions 374
3.4 Data protection in Australia 375
3.4.1 Regulatory and enforcement institutions 377
3.5 Data protection in South Africa 378

4. CHOOSING A DATA PROTECTION MODEL FOR NIGERIA 379
4.1 Government regulation (the command and control model) 380
4.2 Self-regulation 381
4.2.1 Arguments against self-regulation 383
4.3 Co-regulation 385
4.4 Conclusion 385

5. RULES V PRINCIPLES 387
5.1 Rules-based regulation 387
5.2 Principles-based regulation 387
5.3 What to consider in deciding what model to adopt 390

CHAPTER 9: CONCLUSION, SUMMARIES AND RECOMMENDATIONS 393
1 CONCLUSION 393

2 SUMMARIES 396

3. RECOMMENDATIONS 403
3.1 Enact a comprehensive data protection law based on "fair information principles" 403
3.2 Establish a statutory data protection regulatory authority 405
3.3 Education and publicity: The public must be empowered to take actions to protect their personal information 406

3.4 Amend s. 37 of the 1999 Constitution to make the privacy protection guaranteed therein available to all residents and not only citizens of Nigeria. The data protection law should protect the data privacy of not only Nigerians but all residents in Nigeria including those outside Nigeria whose personal data shall be transmitted to Nigeria 407
3.5 Strengthen the Judiciary 408
3.6 The Nigerian Law Reform Commission should conduct further studies and carry out extensive consultations with all stakeholders in the society in order to determine the best regulatory model to adopt 410

BIBLIOGRAPHY 413
Books and journals..... 413
Online / Internet sources 456
Documents issued by International organisations, Data Protection Agencies / Commissioners, Conventions, Directives, Reports..... 497
Newspapers, Magazines, Dictionaries and Encyclopaedias..... 506

TABLE OF CASES 516

TABLE OF STATUTES 522

CHAPTER 1

THE RESEARCH PROBLEM

1. INTRODUCTION

A global information revolution[1] has been underway for the last three decades or more and different countries are staking their claims to the promised benefits of the revolution. Participating in and benefitting from this revolution is largely dependent on a country's networked readiness.[2] In 2002, the Berkman Center for Internet and Society of Harvard University published the first in a series of reports that measured the preparedness of nations to use the enabling technologies of the Internet to leverage their development. In each of the reports, the Networked Readiness Index measures the networked readiness of each country surveyed. The 2002 report surveyed 75 countries, including Nigeria, according to their capacity to use information and communication technologies (ICTs). The Index for 2002 ranked Nigeria 75th, the least ready to participate in the networked world. Subsequent assessments of Nigeria's networked readiness over the years have consistently shown a less than satisfactory state of preparedness to leverage on the advantages of ICTs and the Internet. For example, in the 2007–2008 and 2010-2011 reports,[3] Nigeria

---

1 The Information Revolution generally refers to the dramatic changes that have taken place in virtually every sphere of human activity particularly in the economic sector, from the last half of the 20th century to the present. The phrase is often used interchangeably with Information Age and Information Society. This era is characterised by profound increases in the creation, use, management and dissemination of information aided by computers, telecommunications/mass media and the Internet. This revolution results in increased productivity occasioned by the use of the information technologies. It is a revolution that is based on information and driven by information and communication technologies. According to the High Level Group on the Information Society: "[T]his revolution adds huge new capacities to human intelligence and constitutes a resource which changes the way we work together and the way we live together." See European Commission *Report on Europe and the Global Information Society* (*Bangemann Report)* 10.

2 "Networked Readiness" is defined as "the degree to which a community is prepared to participate in the Networked World." According to the authors, networked readiness is "gauged by assessing a community's relative advancement in the areas that are most critical for ICT adoption and the most important applications of ICTs". See ITG *Readiness for the Networked World* 5 [online].

3 Dutta and Mia *The Global Information Technology Report 2010–2011* 255.

was ranked 94 out of 127 and 104 out of 138 respectively.

With Networked Readiness Index rankings of 75[4] in 2002 and 104 in 2011, Nigeria is but a dot on the global network map. Nevertheless, the country has in recent years been increasingly identified by the dark side of the information revolution. This identification is of a dubious and negative significance, arising mainly from the "exploits" of a small number of the citizens in the matter of email scams, otherwise known as "419" frauds.[5] The migration of the "419 scam" from the post office to cyberspace via the Internet has resulted in an exponential growth of the scam and other computer-aided crimes. This has consequently resulted in a negative perception of Nigeria's interaction with the Internet in particular, and the global economy in general.

The negative perception notwithstanding, the country recognises the need, not only to be represented on the Internet, but to reap the benefits of being plugged into the global networked economy.[6] One of the realities that developing countries like Nigeria have to face today is that national and international markets have become more and more interconnected through the global platform of the Internet. This global networked economy is creating a paradigm shift in the focus of developmental goals and strategies particularly for developing countries.

1.1 The global network economy

Accessing the global market demands a network presence; Nigeria must plug into the network or risk being shut out. However, networks are operated by means of protocols and standards agreed to by the network participants.[7] The global

---

4 Kirkman et al *The Global Information Technology Report 2001-2002* 11.

5 The "419" scam refers to a criminal offence in s 419 of the Nigerian Criminal Code Act Cap 77 Laws of the Federation of Nigeria 1990, which provides as follows:

> Any person who by false pretence, with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

6 See par 1.4.1 below.

7 For example, the Internet operates by the TCP/IP protocols (Transmission Control Protocol/Internet Protocol). TCP/IP is the basic communication language or protocol of the Internet. TCP breaks messages

networked economy has, and is continuing to adopt protocols and standards that demand adherence by those who seek to interact with it. One of the new standards gaining momentum and prominence is data protection. Data protection is part of the law of privacy; its main purpose however, is to "regulate the collection, storage, use and transmittal of personal information"[8] whether the data is collected from the individual or a corporate entity. It is no longer just a constitutional or statutory issue;[9] data protection has become an international trade issue as well.[10] The question that arises for consideration in this thesis is what implications these new protocols or standards have for Nigeria's integration into the global networked economy.

The global networked economy demands that each country seeking to participate in the global network must connect thereto. Developed and developing countries alike are therefore connecting their economic and communication systems to the global

---

transmitted over the Internet into smaller packets and verifies the correct delivery of data from one computer to another. It reassembles the packets of data into the original message and if there is data loss, it triggers retransmission until the data is correctly and completely received. IP handles the address part of the data packets and forwards each packet based on the IP number.

8 Bennett *Regulating Privacy* 13. The right to data protection "establishes and underpins an individual's right to control the storage and circulation of data about himself." See Committee on Data Protection (*Cmnd 7341 para 2.04* 1978) report quoted in Tugendhat and Christie (ed) *The Law of Privacy and the Media* 154.

9 Privacy is recognised as a human right under international law - see art 12 *Universal Declaration of Human Rights* (UDHR) (1948) and art 17 *International Convention on Civil and Political Rights* (ICCPR) (1966). The ICCPR obliges states to enact laws to protect privacy. Many countries and international organisations have incorporated or enacted the privacy provisions of the above international law documents into their national constitutions and charters. See Art 8 *European Convention for the Protection of Human Rights and Fundamental Freedoms* (1950); S 37 Constitution of Nigeria (1999). Although the US Constitution does not contain any express right to privacy, the interpretation of some of the provisions of the Bill of Rights provide protection to some specific aspects of privacy, such as the privacy of beliefs (1st Amendment), privacy of the home against demands that it be used to house soldiers (3rd Amendment), privacy of the person and possessions as against unreasonable searches (4th Amendment). See *Stanley v Georgia* 394 US 557 (1969); *Griswold v Connecticut* 381 US 479 (1965); *Roe v Wade* 410 US 113 (1973). The *African Charter on Human and Peoples' Rights* does not make any provision for privacy.

10 Traditionally, the US has adopted a laissez-faire approach to regulating data; consumer information is bought and sold with minimum state scrutiny or supervision. Europe on the other hand, insists that the consumer have a say in how information about him is used while the state monitors compliance. The 1998 European Union *Data Protection Directive* stipulates that data cannot be transferred from the EU to countries that lack similar standards. According to Singleton:

> It is this component of data protection laws - the determination whether another country's laws are adequate - that transforms data protection laws from domestic matters into international trade issues.

See Singleton *Privacy as a Trade Issue* 2 [online].

market network that makes up the global networked economy. However, none of these national systems is designed and deployed at the global level. Each country builds up its own network and then connects to the global network. In other words, the international economic and communications systems are made up of inter-connected national economic and communications systems. It is the national governments, regional consortia and international organisations that grapple with the task of enacting rules and standards that allow national systems to work together as global systems.[11] According to Regan:

> The global economic and communication systems are fundamentally global information systems. These collect, transmit, exchange and manipulate vast quantities of information, and overcome the traditional barriers to the international movement of information.[12]

These globally networked economic and communication systems have given rise to a significant traffic of personal data which are harvested from the myriads of transactions across different territories and fed into the networks. For example, reserving a flight in Lagos for a journey to London by British Airways will result in the personal data of the passenger being transmitted to London. This trans-border flow of personal data may pass through as many as five or six different countries depending on the telecommunication networks in use. This may ordinarily not elicit any concern, but if on return to Lagos, the passenger begins to receive marketing offers from companies unknown or unsolicited by the passenger, then privacy issues arise.[13]

---

11 Regan 1993 (52) *Am J Econ Sociol* 257.

12 Ibid.

13 This is a phenomenon quite familiar to users of the Internet including users located in Nigeria. You visit one website and are compelled to register by revealing personal information about yourself in exchange for the service sought. From the following day onwards, you become the unwilling recipient of various offers in your mailbox from sources you never even knew existed. For our passenger who did not reckon with unsolicited marketing offers, their presence in his mailbox constitutes at the least, an undesired invasion of privacy. According to one privacy commentator, "[p]rivacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations." See Clarke *Introduction to Dataveillance* [online].

See however Neethling's definition of privacy as "… an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself or herself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he or she evidences a will for privacy."... Neethling, Potgieter and Visser *Neethling's Law of Personality* 32. The authors consider the scenario outlined above not as an invasion of privacy, but as an invasion of another personality interest of the passenger, namely his "feelings". The receiving of unwanted email does not involve an acquaintance with private facts, and therefore in Neethling's opinion

1.2 The trans-border flow of information

The personal data of the passenger in the example given above may flow in a manner similar to what Regan describes; that is, information about an individual is collected in country A, transmitted by a telecommunications network owned and operated by a company in country B, processed in country C, stored in a computerised database in country D, transmitted to country E for analysis, and repackaged and sent to country F for another use. She contends that the six countries the information travelled through may well have different standards of protection for personal information. The result, according to the author is that:

> ... the individual's legal privacy protection changed as the data changed countries and [that] the obligations of the users and disseminators of personal information, primarily multinational corporations, changed as well.[14]

Information is indispensable in modern world economic activities.[15] The technological capacity to collect information, particularly of the personal type, now constitutes the greatest threat to information privacy.[16] Finding a balance between the legitimate need to collect information and the need to protect privacy has therefore become a matter of global concern and a major challenge. Rotenberg predicted a few years ago that "privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century."[17] This prediction is now a reality.

---

does not involve privacy. In the scenario above, the obtainment of the e-mail address without the knowledge or consent of the owner does qualify as a breach of privacy, since the e-mail address contains personal information. In any event, it has been opined that "[I]f privacy is, as Brandeis and Warren defined it, the right 'to be let alone', then the incessant hounding by spammers should be recognized as an invasion of that right." See Hirsch "Is Privacy Regulation the Environmental Law of the Information Age?" 239.

14 See n 11 at 259.

15 Branscomb *Economics of Information* [online].

16 See par 2.2 below.

17 See Gleick "Big Brother Is Us" [online].

1.3 Privacy and data protection after the information revolution

The advent of the Information Revolution with its enabling technologies brings with it the potential for mischief,[18] because information has acquired an economic value `hitherto unrealised. There is, as Leith suggests, a "commodification of information"[19] which is being encouraged by various legislatures across the developed world by according property rights to information which previously had no substantive existence.[20] Thus, the growing importance and value placed on information and ideas in the global information economy, coupled with the fact that these assets are now generally stored electronically, create an increasing need to protect them through legal and other means from unauthorised use and interference.[21]

One of the means of protecting personal information in electronic format is data protection. Data protection laws arose from the realisation in many developed countries that the standards of personal privacy that had been enshrined in constitutional and statutory laws, had become inadequate to deal with the

---

[18] Some of the mischiefs associated with the enabling technologies of the revolution, particularly the Internet, are computer hacking, unsolicited e-mails (or "spamming" which can be either commercial bulk mails made up mostly of advertisements of products and services, or non-commercial bulk mails from private sources such as religious or political groups), theft of passwords and credit card numbers, phishing (an unlawful technique used on the Internet to gain personal information from users of certain websites for purposes of identity theft by using false e-mail messages that appear to come from legitimate businesses; these e-mail messages are designed to deceive recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers), publication of obscene materials, trademark and copyright infringements. In the words of Al Gore: "Unlawful activity is not unique to the Internet - but the Internet has a way of magnifying both the good and the bad in our society…what we need to do is find new answers to old crimes." Vice President Al Gore (Press release August 6 1999), announcing new steps to address unlawful conduct on the Internet.

[19] Leith 1997 *JILT* 2 [online].

[20] In the last two decades the role of intellectual property law has been significantly expanded in the areas of copyright and patent protection to extend protection to items like computer software and software-related inventions. According to Rowland, the initial impetus for the *Database Directive*, (*Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996, on the legal protection of databases* OJ No. L 77/20 1996) was the rapidly growing market in electronic databases made possible by computer technology. See Rowland 1997 (5) *Web JCLI* [online]. See also, the Digital Millennium Copyright Act of 1998 (USA), which confers new rights in copyrighted works, and limitations on those rights, when copyrighted works are used on the Internet or in other digital, electronic environments. See National Research Council *The Digital Dilemma: Intellectual Property in the Information Age* 49 n 3.

[21] Lipton 2001 (6) *J Tech L & Pol'y* 1. This however does not suggest that there is no protection whatsoever; indeed most jurisdictions today, particularly the common law ones of which Nigeria is one, afford remedies for breach of confidence, copyright, defamation and negligence, law of contract on express or implied terms, public interest immunity and legal professional privilege.

technological changes brought about by information and communication technologies (ICTs). This was particularly so with regard to the processing of personal information by the new information technologies.

To remedy the inadequacy, the Organization for Economic Cooperation and Development (OECD), proposed eight information handling principles[22] that will safeguard the privacy of personal information collected, stored and used by the new information technologies. These principles formed the basis for a Convention[23] by the Council of Europe with the aim of protecting individuals in circumstances where information about them is processed automatically. The Convention also seeks to facilitate a common international standard of protection for individuals, so that the free flow of information across international boundaries will not be hindered.

The defining features of the Information Revolution are the acquisition, processing, storage and dissemination of information. Consequently, the Information Revolution has brought new challenges to the protection of people's privacy, because of increased opportunities for privacy violations.[24] This is because the technologies for such acquisition, processing and storage continue to grow in sophistication and efficiency.[25] Information has become a premium commodity, and personal data have become an important subset of information. Governments, industries and the private sector generally collect and use these data for purposes such as marketing, statistics

---

22 OECD *Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data*.

23 Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* CETS No. 108 (1981) which entered into force on 1 October 1985.

24 Spamming (see n 18 above), profiling, data matching, cookies and data mining are some of the methods of violating people's privacy.

25 See eg *Whalen v Roe* 429 US 589, 605 (1976) where Steven J expressed this idea: "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerised data banks or other massive government files". Indeed, the march of civilization and the tools that its technologies produce are implicated in the increasing concern with their capacity to compromise privacy. See eg Warren & Brandeis 1890 (4) *Harv L Rev* 193:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops.

and law enforcement.[26]

The right to privacy[27] is a globally recognised human right; article 12 of the *Universal Declaration of Human Rights* (UDHR) by the United Nations (UN) established privacy as a fundamental human right in 1948.[28] The *International Covenant on Civil and Political Rights* (ICCPR) reinforced the UDHR[29] by specific treaty law.[30] As far back as 1976, the United Nations drew attention to the need for ensuring adequate privacy protections for the "... privacy of the individual in the light of modern recording devices".[31] One of the proposals by the UN Secretary-General arising from the report, was the recommendation that "[s]tates shall adopt legislation, or bring up to date existing legislation, so as to provide protection for the privacy of the individual."[32] Those recording devices contemplated in the UN Report of 1976 have witnessed such technological advancements today that the call for privacy protections, inter alia in the form of data protection laws, resounds in many

---

[26] Solove speaks of "digital dossiers" that are constructed and used through three types of information flows. Information flow is a way of describing information movement and can be:

- Between large computer databases of private-sector companies;
- From government public record systems to a variety of businesses in the private sector (many companies construct their databases by extracting personal data from public records held by governments);
- From the private sector to government agencies and law enforcement officials.

See Solove *The Digital Person* 3. The scenario painted by Solove may be true of the US, but on a smaller scale it is also applicable to Nigeria, particularly in the banking and telecommunications sectors of the economy. In these sectors, companies are required by statute to render returns to the Central Bank of Nigeria and the Nigerian Communications Commission on their operations.

[27] See n 9 above.

[28] The article provides that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

See UN General Assembly *Universal Declaration of Human Rights* (Resolution 217A (III)) 1948. The *International Covenant on Civil and Political Rights* ("ICCPR") art 17 provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

See UN General Assembly *International Covenant on Civil and Political Rights* (*Resolution 2200A (XXI))*1966.

[29] See n 9.

[30] Michael *Privacy and Human Rights* 19.

[31] UN *Doc E/CN.4/1116*.

[32] Ibid.

countries of the world.[33]

1.4 Privacy as an international trade issue

Nigeria cannot afford not to hear the resounding clamour for improved privacy protection across the world today.[34] There is no dedicated data protection law in Nigeria but the Constitution guarantees the right to privacy. Section 37 thereof provides that:

> [t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.[35]

There is clearly a relationship between privacy and data protection. Data protection[36] is subsumed under the right to privacy.[37] The right to privacy is recognised as conferring on the individual the right to control the way his or her personal

---

[33] At the end of 2002, there were 43 nations with enacted Data Protection Laws. (See EPIC & Privacy International *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* iii-iv). Since then however, more countries like Uruguay and Tunisia have joined the list. As of mid-2011, there were 76 countries with enacted data protection laws. See n 877 below.

[34] See UN Doc *E/CN4/1233* (1976); this UN document which is a follow up to Doc *E/CN4/1116* (n 30 above), recommended a number of model provisions for possible inclusion in draft international protocols for privacy. The following provisions are relevant to the focus of this study:

i. The States which have not yet done so should adopt appropriate legislation containing rules relating to computerised personal data systems in both the public and private sectors. As far as possible, legislation should be adopted concerning all types of computerised personal data systems (statistical and research systems, administrative systems and intelligence systems), but may vary according to the nature of those types of systems.
ii. The following minimum standards should be followed in drawing up national legislation:
   (a) only the personal information strictly necessary for the purposes of the respective system should be collected;
   (b) the individual should be notified that information is being gathered about him and his agreement should be obtained before the information is stored, provided that information may be gathered without such knowledge and agreement in areas related to national security, law enforcement and criminal justice and in other areas for which the law has established that such knowledge and agreement are not required due to the purpose of the gathering of information, subject to appropriate safeguards for human rights which should include those suggested in points 3(a)(i) and (iii) and 3(b)(c) in paragraph 177 of document *E/CN.4/1116*.

See n 30 at 21 – 24, where the recommendations of the UN documents *E/CN4/1116* and *E/CN4/1233* (1976) are reproduced.

[35] Constitution of the Federal Republic of Nigeria (1999).

[36] See n 8 above.

[37] See n 9 above.

information is collected and used.[38] Data protection, by establishing an individual's right to control the storage and circulation of data about the individual, is one of the means by which the right to privacy is protected.

The question arises whether Nigeria's constitutional guarantee of privacy also includes data protection and if it does, whether the protection is adequate in the light of current global trends in data protection enactments. It should be pointed out that this global trend is partly in reaction to the European Union *Directive* on data protection[39] which restricts the transfer of personal data to third countries that do not provide "adequate level of protection" of data privacy rights.[40]

In 2001, Nigeria set for itself the ambitious goal of being a key player in the Information Society by the year 2005. Although this goal was not realised in 2005 and has in fact not been realised so far, it remains to be said however, that the country has made tremendous progress towards realising the goal. The national policy document on IT noted that a developing nation like Nigeria, aspiring "to participate effectively and become a key player in the emerging Information Age"..."needs to have in place, a highly efficient Information Technology system..." as the "engine for sustainable development and global competitiveness".[41] Sustainable development and global competitiveness imply, and indeed require active participation in global trade that is increasingly being dictated by norms set by external powers and factors.[42] For example, under the Lome IV Convention between

---

38 See Westin *Privacy and freedom* 7.

39 *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*, (hereinafter the *Directive 95/46/EC*). The *Directive* which came into force on Oct. 24th 1998 has two major objectives: (1) the protection of information privacy by Member States of the EU; and (2) the prevention of restrictions on the free flow of personal information among EU Member States, for reasons of privacy protection. In other words, by establishing a clear and stable regulatory framework that requires a uniform minimum standard of privacy protection across the EU, the *Directive* aims to ensure both a high level of protection for the privacy of individuals in all Member States and the free movement of personal data within the EU. See Articles 1(1) and 1(2) of the *Directive*. See also Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 189 for a discussion of the *Directive*.

40 Id art 25 (1).

41 NITDA *National Policy for Information Technology* ii-iii [online].

42 See n 44 below.

the European Union and the African, Caribbean and Pacific (ACP) states,[43] the protection of human rights within the territory of the parties to the Convention has become a matter of common concern.[44]

It is arguable that the EU *Directive 95/46/EC* on data protection has introduced the notion of human rights into the international trade arena because European states treat privacy as a political imperative anchored in fundamental human rights.[45] The aim of the *Directive* is to enhance trade in the European Union by harmonising information privacy rules within the Union, thus removing a potential trade barrier arising from conflicting information privacy protection rules.[46] While the *Directive* seeks to remove a potential trade barrier between EU members, it implicitly sets up a potential barrier between the EU and third countries in relation to their domestic privacy regulatory regimes if they fail to meet European standards.

Nigeria has a significant trade relationship with the EU; statistics for 2010 show that Nigeria's trade with the EU constituted 25.3% of its total world trade. A significant portion of this trade is in oil and gas, but also includes other sectors such as the services and industrial sectors.[47] It is inevitable that the trade relationship will necessitate the transfer of personal information between the two trading partners,

---

43 See the ACP-EC website [online]. Nigeria is a member of the ACP-EC.

44 In the Agreement amending the fourth ACP-EC Convention of Lome signed in Mauritius on 4th Nov. 1995, the amended art 5 provides *inter alia*:

> 1. Cooperation shall be directed towards development centred on man, the main protagonist and beneficiary of development, which thus entails respect for and promotion of all human rights. Cooperation operations shall thus be conceived in accordance with this positive approach, where respect for human rights is recognised as a basic factor of real development and where cooperation is conceived as a contribution to the promotion of these rights… Respect for human rights, democratic principles and the rule of law, which underpins relations between the ACP States and the Community and all provisions of the Convention, and governs the domestic and international policies of the contracting parties, shall constitute an essential element of this Convention.

Quoted in Wyatt *Freedom of Expression in the EU Legal Order and in EU Relations with Third Countries* 217. Wyatt asserts that "[t]he role of the European Parliament in addressing and seeking to address the grievances of citizens of the Union may overlap with its role in reviewing alleged violations of human rights by third countries committed to human rights protection by their treaty relations with the European Community" at 219. See the *Agreement Amending the Fourth ACP-EC Convention of Lomé* 1995.

45 Reidenberg 2001 (38) *Hous L Rev* 731.

46 Shaffer 2000 (25) *Yale J Int'l L* 11.

47 The European Union *Trade with the World and EU Trade with Nigeria* [online].

particularly in the services sector. The adequacy of Nigeria's level of data protection will thus become an issue and potential trade barrier. The volume of trade with the EU is significant enough to adversely affect Nigeria's economic interests if there is any disruption of trade due to a finding of inadequate data protection in Nigeria. It follows therefore, that Nigeria's integration into the global networked economy requires a legal and regulatory infrastructure that meets international standards and benchmarks that recognise privacy as a trade issue.

Globalisation is driving the nations of the world more into political and economic integration.[48] These integrations are enhanced by a globally interconnected network of economic and communication systems at the apex of which is the Internet. This network of networks thrives on and encourages the expansion of cross-border flows of ideas and information, goods and services, technology and capital. The speed and efficiency of data processing and transmission make the transfer of data across borders very easy. The Internet provides the latest and perhaps potentially the biggest marketplace in the history of commerce.[49]

In order to provide a stable, secure and trustworthy environment for conducting business in this new marketplace, consumer protection has become critical. In many developing countries however, laws governing communication and storage of information specifically, and commercial law rules in general, are inadequate to address transactions in the electronic medium in national or cross-border commerce. This inadequacy presents real and potential barriers to the use of the modern electronic medium for trade.[50] If a country ignores this reality, it risks being "unplugged" from the global networked economy.

Information is the currency of the New Economy that the Information Revolution has

---

48 Examples of such integration are the European Union (originally EEC formed in 1957, became EU in 1992), the African Union (originally OAU formed in 1963, became AU in 2002), North American Free Trade Agreement (NAFTA) (1994), and Economic Community of West African States (ECOWAS) (1975), Southern African Development Community (SADC) (formerly SADDC, 1980).

49 UNESCO *World Communication Report: The Media and the Challenges of the New Technologies* 47.

50 See UNCTAD *The Digital Divide: ICT Development Indices 2004* 1. According to the report, one of the most important factors hindering developing countries from achieving maximum economic potential from ICT includes the absence of adequate legal and regulatory frameworks, among other factors.

given birth to. Enabling access to information technologies will enhance the productive capacities of the different sectors of Nigeria's economy.[51] Productivity and competitiveness are now based on knowledge and information, powered by information technology. This translates essentially into the need for a technological infrastructure in which highly educated and skilled human resources will play a crucial role.[52]

1.5 Getting Nigeria "connected" to the Global Network Economy

Nigeria is adjudged to be one of the least networked nations in the world. In any discussion about data protection, trans-border data flows or information privacy (as in this study), the assumption is that there is a significant presence or interaction with a networked environment. A networked environment is "... the one with the most highly developed ICT networks and the greatest potential to exploit those networks' capacity."[53] The quoted definition of networked environment is contained in a world-wide survey of different countries' network capacities. The first survey, which covered the period 2001-2002, yielded a Networked Readiness Index ranking of 75 for Nigeria. In contrast, Malaysia, a country which gained independence the same year as Nigeria, recorded a score of 36 in the Index for the period 2001-2002. With such unimpressive figures, it would not be out of place to ask why Nigeria should bother with high technology-related issues such as data protection/information privacy and trans-border data flows.

The answer could be found partly in the observation of Mowlana that:

> A new power structure is emerging based on information, data and knowledge and leaving behind it levelling effects on traditional and existing social strata. Many decisions affecting the global socio-cultural

---

51 UNDP *National Human Development Report* 20.

52 Ibid.

53 See n 3. The report shows that in the year 2000-2001, Nigeria, with a baseline estimate of 114 million people had:

i. Internet hosts per 10,000 people……..……..0.06%
ii. Personal Computers per 100 inhabitants……...0.61%
iii. % of PCs connected to the Internet…….. 0.01%
iv. Internet users per 100 inhabitants……. 0.09%

The latest ranking, released in the 2012 Networked Readiness Index, shows a significant decline in Nigeria's ranking, from 75 to 112. See World Economic Forum *Global Information Technology Report 2012* [online].

> environment are now largely occurring outside local and even national political and economic systems. Not only are communication networks as cultural ecology affecting the socio-cultural environment, but information and cultural relations are becoming ever more central to the conduct of international and global systems.[54]

It stands to reason that a developing country like Nigeria needs to plug into the global networked economy by utilising the Internet and all its enabling technologies.[55] However, this will require the provision of an institutional, financial, social, and regulatory environment that supports and enhances access by the people of the country. Not only the infrastructures, but also the national regulatory frameworks must be internationally compliant and enhance the regulation of trade and investment, intellectual property rights and the privacy of the citizens.

The imperatives of globalisation and the push towards trade liberalisation and deregulation now compel developing nations like Nigeria to take adequate measures to attract the inflow of trade and foreign direct investment. For example, the inflow of foreign direct investment cannot be assured in an environment where the legal system cannot or does not adequately protect property rights. At the minimum, measures such as the protection of lives and property, contractual rights and, as is now seemingly inevitable, enhanced right to privacy are required in order to participate in and benefit from the global networked economy.

These measures or standards are set by the major players in a globalised and networked marketplace such as the US and the EU. How far Nigeria has gone in meeting these minimum measures, with particular emphasis on privacy, will be the focus of this thesis. Regardless of Nigeria's low network presence, it trades and interacts with the other countries that are very visible on the global network. It sends and receives data to and from these countries. The fact that Nigeria's high ambition to be a key player in the international society lies in sharp contrast to her low network capacity, compels a study of the impacts that trans-border data flows and data protection issues from other countries will have on the stated ambition.

---

54 Mowlana *Global Information and World Communication* 204.

55 Ndukwe *Challenge of Globalisation* 3-5 [online].

1.6 New norms for the digital world

With the onset of the Information Revolution worldwide, there has arisen, on a near global scale, an emerging legal order of laws and norms for a new digital world. These laws and norms are being fashioned out of the conflicts and tensions that are daily being thrown up by the players and dynamics of the digital environment.[56] As these conflicts have arisen, the need to resolve them has often led to new laws related to and reflecting the peculiar nuances of a globally connected world. The ways various state jurisdictions have perceived, responded to or resolved these conflicts have been understandably different. There is a shift from unilateral to multilateral initiatives, often times under the aegis of the United Nations and other supranational or inter-governmental and non-governmental organisations.[57] These efforts seek to fashion out appropriate responses to particular legal issues arising from or particularly affected by the Information Revolution. A case in point is the European Union's responses to various issues arising from the increasing reliance on information and communication

---

[56] Trans-national conflicts have often been resolved through the harmonisation of laws. With regards to the digital environment as exemplified by the Internet, there have been initiatives emerging from the United Nations, the Council of Europe, the Organization for Security and Cooperation (OSCE) in Europe, and the G8 industrialised countries, aimed at dealing with these conflicts and differences in legal responses. Some of the outcomes of these collaborations include:

- UN *Convention against Transnational Organised Crime*; Resolution 55/25 of the General Assembly (2000).
- Council of Europe (CoE) *Convention on Cybercrime* (8 November 2001). This is the first international treaty on crimes committed via the Internet and other computer networks.
- EU Commission *Proposals for a Council Framework Decision on attacks against information systems* (2002). Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981).
- European Union *Directive 95/46/EC of the European Parliament and of the Council, on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data* (1995).
- UNCITRAL *Model Law on Electronic Commerce* (1996). Being a "model" law, it is presented as a "framework" law that should be supplemented by technical regulations formulated by the enacting state. It does not set out all the rules and regulations that may be necessary to implement the use of modern telecommunications for recording and communicating information in various types of circumstances in the enacting state.
- WTO *General Agreement on Trade in Services* (GATS).

In recent times, the World Summit on the Information Society (WSIS) can be seen as a global meeting point for information sharing on how to effectively regulate economic, social, and criminal conduct across borders. The first phase of WSIS took place in Geneva hosted by the Government of Switzerland from 10 to 12 December 2003, where 175 countries adopted a *Declaration of Principles and Plan of Action*. The second phase took place in Tunis from 16 to 18 November 2005.

[57] Ibid.

technologies. The Union has responded by spelling out the rights and duties of all users and providers of these technologies and state authorities in the Union by way of Directives.[58]

The ever-expanding flow of personal data through telecommunications networks and the Internet is one of the most significant public policy concerns spawned by the Information Revolution. More than any other single factor, computers and the networks that connect them have dramatically expanded both the practical ability to collect and use personal data and the economic incentive to do so. Samuelson is right in asserting that:

> Information privacy is a social goal, not a technological one. To achieve information privacy goals will require social innovations, including the formation of new norms and perhaps new legal rules to establish boundary lines between acceptable and unacceptable uses of personal data.[59]

1.7 The right to know (freedom of information) and the right to hold back information (privacy)

The social innovations and formation of new norms arising from the impact of the new technologies in the last decade, particularly in the technologically developed countries, have given rise to a robust advocacy agenda that seeks greater protection for privacy rights. In Nigeria however and prior to 2011, the struggle was focused more on getting access to information than to information privacy. It would not be far from the truth to say that information privacy is a relatively novel idea in Nigeria: many of the users of technology in the country are not aware of their privacy-intrusive capabilities. Herein lies the dilemma of the Nigerian society in the Information Age – the struggle between the right to know and the right to hold back information. With regard to the right to know, Nigerians are information poor and the struggle for access to information has been long and arduous.[60] This is due in

---

58 See for example, n 39. Another example is the *Directive 2002/58/EC.*

59 Samuelson 2000 (52) *Stan L Rev* 1125 at 1169.

60 In September 2004, the House of Representatives, the lower chamber of the bi-cameral National Assembly, passed the Freedom of Information Bill. Shortly thereafter, the Senate received a copy of the passed Bill for its consideration and passage. From then on, the FOI initiative suffered a number of

part to the poor level of literacy,[61] and to the high cost of acquiring the means of sourcing information such as radios, televisions, telephones, computers and even newspapers.

In the main, this poverty of information is the result of the government keeping information from the reach of the people. Virtually all government information in Nigeria is classified as 'Top Secret', save such as the government determines to be safe to release to the people. However, this is not peculiar to Nigeria. As indicated by the Commonwealth Human Rights Initiative (CHRI), "[u]nfortunately, the assumption that information is secret has always been a major premise of the relationship between ruler and ruled in the Commonwealth."[62] The resulting struggle for information[63] is in response to this false assumption that information must be kept secret; this assumption has worked against having a robust privacy advocacy focus in Nigeria. A society long used to fighting for information to be free and easily accessible, will not easily warm to the idea of information privacy. It will see such advocacy as seeking to make information inaccessible again. This will create tension between the right to know (freedom of information) and the right to hold back information (information privacy). This tension is understandable in the light of some of the consequences of withholding information such as corruption.

A plethora of laws and regulations prevent government functionaries and institutions from divulging information which properly ought to be in the public domain in Nigeria. The single most notorious culprit for this information blackout in Nigeria is the Official Secrets Act.[64] The culture of secrecy that the Act engenders and the veil of secrecy that permeates the fabric of governance are some of the reasons why

---

legislative setbacks until it was finally passed by the Senate in 2011. The FOI initiative started with the 4th National Assembly (1999-2003) when it was first introduced and was eventually passed by the 6th National Assembly (2007-2011). The Act was signed on 28th May 2011. For a succinct account of the FOI Act journey, see Odinkalu *Nigeria's Freedom of Information Law: How Friends Launched a Movement* (2011).

61 Nigeria's literacy rate is said to be 68% for those from15 years and above. See CIA *World Fact Book* (2011) [online].

62 CHRI *Looking for the Right to Information in the Commonwealth* 11 [online].

63 See chp 5 par 1.3 below for a fuller discussion of the struggle for information in Nigeria.

64 Laws of the Federation of Nigeria 1990 Vol 15 Cap 335.

corruption and maladministration thrive in the country. The CHRI noted in its Report for 2003 that:

> A guaranteed right to access information is an essential and practical antidote to corruption which is rife in too many Commonwealth countries. Corruption is destroying the rule of law and has created a mutually supporting class of overlords who need secrecy to hide their dark deeds in dark places.[65]

The tension between privacy and freedom of information has always been played out in different societies. For Nigeria, this interplay takes place against the backdrop of an endemically corrupt society in desperate need for solutions to the malaise. Access to information is a powerful antidote and crucial for exposing corruption. Until recently in the history of Nigeria, that access was simply not there. Perhaps now that the Freedom of Information Act[66] has been enacted, the suggestion that Nigerians be invested with legal right to control access to their personal information by means of a data protection law will no longer be seen as an obstruction to the freedom of information.

The fight against corruption can negatively affect the drive for information privacy by pressuring governments into enacting laws that deprive its citizens of their information privacy rights. The international financial community has systematically applied pressure upon Nigeria to rein in the pervasive incidences of financial and economic crimes in the country.[67] It was in the face of such pressures and in response to calls from governments across the world that Nigeria's President Olusegun

---

65 See n 62 at 21.

66 The Act is available on the website of the Freedom of Information Coalition. Also see Freedom of Information Coalition *Memorandum on the Freedom of Information Bill* [online].

67 Nigeria was placed on the Financial Action Task Force on Money Laundering (FATF) List of non-cooperating states from 2000 to 2006 when it was delisted. During the period it was on the list, the country suffered the imposition of counter measures applied as sanctions against it. See FATF *Annual Review 2006-2007* [online]. Regarding corruption, Transparency International (TI), in its *Corruption Perception Index* [online], ranked Nigeria 142 out of 163, indicating Nigeria as one of the most corrupt nations in the world. The US Federal Bureau of Investigation placed Nigeria at the forefront of multifarious cyber-crime activities (see FBI *Internet Fraud Report 2001/2002*) [online]). A major consequence of all these pressures is that Nigeria is not attracting as much Foreign Direct Investment (FDI) as it potentially ought to. Business prospects from Nigeria undergo extreme due diligence which add to the overall cost of doing business in Nigeria and it is therefore not an attractive destination.

Obasanjo set up the Nigerian Cybercrime Working Group (NCWG)[68] in 2004. The NCWG was instructed to look into the issue of illegal activities on computer networks and systems, especially the Internet, and to propose a national solution that would restore international commercial trust in Nigeria. The NCWG presented to the government a proposed legislation to combat cyber-crime and other computer-related offences. However, the draft Bill gives cause for concern since it raises privacy issues arising from a data retention provision that is *prima facie*, imprecise and therefore capable of abuse.[69] The pressure to restore the international community's confidence in Nigeria's commercial activities, also presents to the government the temptation to "cut corners". This happens when the government fails to strictly observe the rules in law enforcement and crime detection. In such an environment, privacy interests are greatly at risk.

In a world that is gripped by the spectre of global terrorism and cyber-crime, the choice to withhold personal information is often viewed with suspicion.[70] Protection

---

[68] The NCWG is an inter-ministerial body consisting of law enforcement, intelligence, security as well as ICT agencies of government, plus key private sector ICT organizations. It was established by the Federal Executive Council (FEC) in March, 2004 to, amongst other things, create the legal and institutional framework necessary for securing computer systems and networks as well as protecting critical ICT infrastructures in the country.

[69] The proposed Bill is for an Act "to secure computer systems and networks and protect critical information infrastructure in Nigeria by prohibiting certain undesirable computer-based activities and for matters connected therewith". The Draft Bill, *The Computer Security and Critical Information Infrastructure Protection Act* 2005, [online] was placed before the Senate, the upper chamber of the legislature in 2005. Of particular relevance to the issue under discussion is the proposal for data retention in s 11 which will require ISPs and telecommunication operators to store customer's "traffic, subscriber information or any specific content on its computer or computer network for such period of time as the President may, by Order published in the Federal Gazette, specify from time to time".
S 11(4) thereof provides that:

> Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act or pursuant to any regulation under this section, shall not be utilized except for legitimate purposes. Under this Act, utilization of the data retained, processed or retrieved shall constitute legitimate purpose only with the consent of individuals to whom the data applies or if authorized by a court of competent jurisdiction or other lawful authority. [Underlining supplied]

However, the fact that clear rules defining the circumstances and conditions for derogating from the data owner's refusal of consent are not spelt out in the proposed law, or any regulation, leaves the proposed data protection clause vague and therefore open to abuse.

[70] S 12 of the Advance Fee Fraud and Other Fraud Related Offences Act 2006 requires Internet service providers (ISPs), GSM service providers and other Private Telecommunications Operators (PTOs) that offer Internet services on their networks to register with the EFCC and maintain a register of all fixed line customers which shall be made available for inspection by any authorised official of the Commission. S 13 of the Act sets out the obligations of telecommunications, Internet service providers and Internet Cafes by making them responsible for surveillance of their customers' activities on the Internet. Customers and subscribers who decline to provide or provide false identities and addresses to the service providers are liable to imprisonment for one year on conviction.

from unwanted publicity is perceived as a derogation of the right to freedom of speech and of the press. This is nothing new; sixty four years ago, Arndt contended that "[t]he cult of privacy seems specifically designed as a defence mechanism for the protection of anti-social behaviour."[71] This is one argument that resonated very well with the advocates for "freedom of information" legislation in Nigeria. They argued that the garb of secrecy that adorns most of the acts of corruption and maladministration is bad enough and does not need further help from a regulatory regime that may wittingly or not, assist in the further cover-up of misdeeds in the society.[72]

The news media, the principal proponents of the freedom of information legislation, are concerned that the restrictions that a vigorous privacy regime would impose, could undermine freedom of information and freedom of expression and inhibit the discovery and disclosure of the truth. As a result, they argue, the efforts to battle crime and corruption would be a mirage. This view, plausible as it sounds, assumes the primacy of freedom of expression over privacy which is not supported by the constitution.[73] Under the Nigerian Constitution, freedom of expression is not superior to the right to privacy.[74]

With their capacities not only to enhance the acquisition, storage and dissemination of information, but also to intrude upon the privacy of the users, ICTs present a double-edged sword of opportunity. On the one hand,

> ... [i]mproved and cheaper telecommunications could generate rural employment, could enhance the integration of the rural with the national economy, improve living standards, ameliorate feelings of isolation, and potentially stem the steady migration of people from the countryside to

---

71 Arndt 1949 (3) *Aust Q* XXI 69-71. See also Posner 1978 (12) *Ga L Rev* 399, echoing similar sentiments in his assertion that:

> Much of the demand for privacy… concerns discreditable information concerning past or present criminal or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is… to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit.

72 See, eg Obi, Udonquak and Majekodumi 07 June 2011 *Businessdayonline*.

73 See s 17(2)(a) Constitution of the Federal Republic of Nigeria 1999.

74 The tensions between the right to know and the right to privacy will be further explored in chapter 5.

the cities.[75]

On the other hand, it has been asserted that:

> … [t]he practice of routinely holding information away from the public creates "subjects" rather than "citizens" and is a violation of their rights. This was recognised by the United Nations at its inception in 1946, when the General Assembly resolved: "Freedom of Information is a fundamental human right and the touchstone for all freedoms to which the United Nations is consecrated".[76]

Managing the opportunities for benefits and the temptations for abuse resulting from the new technologies are major challenges for all societies today. For many of these societies, it is inevitable that personal data is disclosed to facilitate various types of transactions, and in a good number of instances, the disclosure is voluntary. However, in an increasing number of cases, such personal data are acquired without the knowledge and consent of the data subject, for example by means of cookies, spyware, adware and keystroke loggers.[77] It is certain that as more developing societies take up the new technologies, occasions for disclosure of personal information will increase and Nigeria will be no exception. This trend will no doubt pose some challenges for the country as it seeks to integrate into a networked global economy. Froomkin, for example, argues that the law should facilitate information privacy and the most effective way of protecting information about oneself is not to disclose it in the first place.[78] This may be true, but it is not always feasible in today's

---

75 Panos Institute *The Internet and Poverty: Real help or real hype?* [online].

76 See n 62 at 12.

77 The data subject is the person to whom the information collected refers; "cookies" are bits of data that a web surfer's browser allows a visited website to write on his hard drive usually without the surfer's knowledge It is a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a Web site server, and containing personal information (as a user identification code, customized preferences, or a record of pages visited). See *Merriam Webster Dictionary* 2010; "spyware" as the name suggests, spies on the user's computer and sends back information to whoever planted it; "adware" is an advertising software usually bundled with a downloaded programme and sends back information to the programme developer or sponsor; "keystroke loggers" are surreptitiously installed by a hacker to record every keystroke that a computer user executes. These are all deceptive programmes that collect data from a user's computer without his knowledge or consent and often for profit motives. See generally, *Encyclopædia Britannica* (2010).

78 Froomkin 2000 (52) *Stan L Rev* 1464.

world. Adequate measures should therefore be taken to safeguard privacy. The responsibility for addressing the privacy protection issues rests primarily with the government.[79]

Notwithstanding that section 37 of the Nigerian Constitution guarantees the privacy of citizens,[80] the desire to keep one's information private has often clashed with the equally compelling need to disclose information. This need underlines the freedom of information movement around the world. The clash will continue until a balance is struck between the right to seek and obtain information on the one hand, and the right to withhold personal information on the other.[81] The very process of striking the needed balance has proven to be problematic, because often it has resulted in preferring one right to the other, usually in favour of the right of expression.[82] This is the situation in the US.[83]

It is not altogether clear whether the same can be said for Nigeria; privacy rights and interests with regard to information do not at present appear to enjoy wide recognition and acceptance. This is not to suggest that there is no provision for such

---

79 See chp 3 par 5.5 below.

80 See n 73. The right to privacy in Nigeria is not absolute; section 45 of the Constitution makes provision for restriction on and derogation from fundamental human rights.

81 *Venables v News Group Newspapers* (2001) Fam 430.

82 Freedom of expression is a fundamental human right; art 19 ICCPR provides that:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

Freedom of information is understood as "the right to access information held by public bodies." See Mendel *Freedom of Information: A Comparative Legal Survey* 14 [online].

83 According to Cate and Litan: "The Supreme Court has decided many cases in which individuals sought to stop, or obtain damages for, the publication of private information, or in which the government restricted expression in an effort to protect privacy. Virtually without exception, the Court has upheld the right to speak or publish or protest under the First Amendment, to the detriment of the asserted privacy interest….The historical dominance of the free expression interests over the privacy interests is so great that Peter Edelman has written:

> [T]he Court [has] virtually extinguished privacy plaintiff's chances of recovery for injuries caused by truthful speech that violates their interest in nondisclosure. . . . If the right to publish private information collides with an individual's right not to have that information published, the Court consistently subordinates the privacy interest to the free speech concerns.

Free expression has trumped privacy under the First Amendment irrespective of whether the speaker is an individual or an institution." See Cate and Litan 2002 (9) *Mich Telecomm & Tech L Rev* 35.

rights.[84] However, in an environment where the need to secure access to information for economic development and to combat crime is only beginning to receive attention from the governing elite, a robust privacy rights agenda is readily dismissible as counter-productive to the fight to secure information access. Law enforcement, whether civil or criminal, relies on information which is often "private" in the sense that it rests in the hands of someone who would like it to be kept secret.[85]

2. IDENTIFYING THE ISSUES AND THE CRITICAL QUESTIONS TO BE ANSWERED

2.1 Relationship between information privacy and data protection

The international discourse on privacy has from inception proceeded along two main conceptual parameters, each with its own preferred nomenclature. In the US, the discourse began in 1890 with the epochal article, "The Right to Privacy",[86] and as a consequence, the terminology of "Privacy" was adopted. Public, academic and judicial debate over the concept of "privacy" accelerated in the 1960s in reaction to the then growing computer industry and the capabilities of the computer to process personal information. The concept of "information privacy" came to the fore during this time.[87]
In Europe, the same fears were expressed but preference was given to "data protection", perhaps because of the more diverse spread of languages. Bygrave traces the nomenclature to the German term "Datenschutz".[88] Both concepts, information privacy and data protection, however, refer to the same core values and interests, not only in the US and Europe, but also worldwide. Moreover, one common quality holds them all together and that is the fact that both suffer from definitional challenges.[89]

---

84 Eg s 37 Constitution of the Federal Republic of Nigeria 1999.

85 Stuntz 1995 (93) *Mich Telecomm. & Tech L Rev* 1016.

86 Warren and Brandeis 1890 (4) *Harv L Rev* 193.

87 See par 3.5 below for an explanation of the distinction between information privacy and data protection. The diminished ability of the individual to control access to, collection of and use of his or her personal information by others gave rise to the recognition of a right of information privacy. See Solove and Rotenberg *Information Privacy Law* 1.

88 Bygrave 2004 (47) *Sc St L* 319-348.

89 See Chp 4 par 1.1.2 below for a brief analysis of the varying definitions of privacy.

2.2 Information privacy in the ICT environment

The adoption and application of ICTs in Nigeria is much more widespread in the telecommunications and financial services sectors of the economy. It is especially in these spheres of activities that personal information of the users of the technologies are collected. The corporate entities that collect personal information also have the capability to distribute or disclose such information to third parties without the knowledge or consent of the user or data subject. As the uptake of technology increases in Nigeria, the individual's ability or capacity to control how his personal information is collected, processed and disclosed is seriously eroded. It is inevitable that personal information is disclosed to facilitate the necessary transactions. The opening of bank accounts, getting driving licenses and other similar transactions elicit the voluntary disclosure of personal information. However, in an increasing number of cases, such disclosure is either deceptively or unobtrusively obtained without the knowledge or consent of the person concerned.[90] The collection of personal information by ICTs calls to question the adequacy of extant laws in Nigeria to protect transaction- generated personal information.

Whilst the rapid development of the new Information and Communication Technologies (ICTs) have had a number of beneficial consequences, such as the rapid increase in telephone density in Nigeria, this study is concerned with the fact that the human rights implications (particularly concerning privacy) of a wholesale adoption of these technologies and their capacities to intrude upon the users' privacy have so far failed to receive adequate or any attention at all in Nigeria. There is a dearth of information and research both from the government and from academia touching upon the interplay between technology and the fundamental rights of the people. It is this concern that informs this research.

[90] *Gordon Kaye v Andrew Robertson and Sport Newspapers Ltd* (1991) FSR 62. In this case, information about the plaintiff, a television celebrity, was deceptively obtained by a journalist without the consent of the plaintiff.

2.3 Data protection and Trans-border Data Flows (TBDF)

The trend towards an international harmonisation of domestic data protection laws provides a particularly compelling reason for examining the issues relating to data protection[91] in Nigeria. This is all the more necessary because at the international level, trade issues are increasingly turning away from commodities, the main source of comparative advantage for developing countries, to trade in services. The developed countries control this sector of world trade and set the terms for trade which others must follow.[92] The convergence of computers with communications networks has had a huge impact on world trade. According to Braga, the impact of information technology on trade in services has led to the introduction of new products such as financial derivatives, computer reservation systems for airlines and telemedicine, as well as qualitative changes in the provision of existing services such as distance education which are powered by technological advances in information technology.[93] The cross-border flow of information is indispensable to these services and they account for a significant portion of trans-border data flow in world trade. The regulation of cross-border flow of traffic whether of goods, services or information is largely controlled by large trading blocs like the EU and the US; the rest of the world can either comply with the terms of the trade or be shut out. Nigeria cannot afford to ignore such developments. However, the question arises whether the EU's threat, implicit in its Directive, to restrict the flow of information to third countries whose data protection levels are considered inadequate, is against WTO rules and its *General Agreement on Trade in Services* (GATS). This issue will be considered in chapter 7.

---

91 See par 2.1.

92 See n 46. A state's large market provides it with leverage on other states' domestic policies because their access to its market is important to them. Shaffer refers to this as "market power" because it derives from the threat, implicit or explicit, of a denial of market access. The combined market power of the European Union is so enormous that it can leverage domestic policies in other economic giants like the USA and more so the smaller and economically weaker nations. The EU Directive implicitly or explicitly threatens a denial of market access to those nations that do not meet the adequacy test on data protection and since many of the developing nations have not enacted such laws, they are more at risk depending of course on if their level of trade with the EU is big enough to warrant such a concern.

93 Hoekman and Braga *Protection and Trade in Services* 4 [online].

2.4 Critical questions to be answered

The global trend referred to above has implications for Nigeria and raises a number of questions which this thesis seeks to answer. Some of the specific questions that will be addressed are:

- Whether a vigorous privacy protection regime would undermine the freedom of information and thereby inhibit the discovery and disclosure of the truth in a manifestly corrupt society;
- Whether the constitutional protection of privacy and statute law at present is sufficient for the protection of information privacy in Nigeria;
- Whether the EU *Directive on Data Protection* requires any response from Nigeria, and if Nigeria does not respond to the Directive's requirement for adequate data protection laws, what the consequences will be;
- Assuming that there is a compelling need to protect, or rather strengthen the protection of information privacy in Nigeria, to explore what approach or model of protection should be adopted.

2.5 Assumptions

Implicit in the perspective of this research is the assumption, on the one hand, that technology is a necessary adjunct to national development in Nigeria, but, on the other hand, that privacy is a human right, the importance of which must not be undermined in the inexorable march of technological advancement in Nigeria.

This thesis will therefore proceed on the following premises:

- The Global Network Economy that the ICTs have given birth to is increasingly being governed by new rules in an emerging legal order that transcends geographical boundaries.
- To be a meaningful participant in this New Economy, each nation must agree to abide by these emerging norms and rules in order to minimise conflicts and maximise benefits.
- The chief currency of this New Economy is information in its different manifestations and it must be allowed to flow freely through the ICTs that make up the international communications network. This freedom of movement must however take account of the compelling demands of privacy.
- To achieve this, each nation must put in place within its own national

jurisdiction, a legal framework that is supportive of the new and evolving legal order and its norms, from which the New Economy is expected to derive its legality, certainty and continuance. It is accepted that different nations have different conceptions of privacy and how it should be protected. Nevertheless, harmonisation between information privacy laws is needed in order to allow free flow of information between different jurisdictions.

3. DEFINITIONS OF KEY TERMS

Various terms such as "Information Revolution," "Information Age", "Information Society", "New Economy", "data", "information", "data processing", "data protection" and "Trans-border data flow" have been used thus far and require clarification. Even though precise definitions may not be possible for some of these terms, they do convey a sense of the importance that information has assumed in human societies today. These terms have frequently been used interchangeably and not surprisingly so, because they all denote the creation, manipulation and use of information, particularly in the creation of wealth. These concepts will be used frequently in the course of this research.

3.1 "Information Revolution", "Information Society", "Information Age"

The "Information Revolution" generally refers to the dramatic changes that have taken place in virtually every sphere of human activity particularly in the economic sector, from the last half of the 20th century to the present. The phrase is often used interchangeably with "Information Age" and "Information Society". It is characterised by the dramatic increase in the creation, use, management and dissemination of information aided by computers, telecommunications/mass media and the Internet. The use of information technologies results in increased productivity. It is a revolution based on information and driven by ICTs.[94]

[94] See n 1.

3.2 "New Economy"/ "Information Economy"

According to Samuelson and Varian,[95] the term "Information Economy" dates back to the 1980s when it referred to an economy driven by services rather than manufacturing. In 1996 however, Michael Mandel published an article in *Business Week* called "The Triumph of the New Economy"[96] which emphasised the development of a technology-driven, fast-growing, low-inflation economy, which he referred to as "the New Economy". This New Economy is characterised by three interrelated features: (i) information, (ii) networking (powered by the Internet), and (iii) globalisation. The term "Information Economy" is often used interchangeably with "New Economy". The New Economy (or Information Economy) is clearly an outcome of the Information Revolution.[97]

3.3 Data

Data are raw facts and figures; by themselves they are not immediately useful until they are put in context by means of processing. Typically data are processed when the data are fed into a computer (called input), where they are stored and processed before they are transmitted to a human or another computer (called output). During data processing, computers are simply used to transform facts from one medium to another. Data processing may involve several stages in which case the "processed data" from one stage may be considered the "raw data" of the next.[98]

---

95 Samuelson and Varian *The "New Economy"* 1 [online].

96 Mandel 30/12/96 *Businessweek*.

97 Ibid.

98 Perrolle *Computers and Social Change* [online].

3.4 Information/personal information

Once data has been given meaning and context by means of processing,[99] it becomes useful information such as audio/video, graphic, numeric or text data.[100] Computers produce information when they store, retrieve, or rearrange relationships among data. For example, a telephone book contains data representing the names, addresses, and telephone numbers of people in a region which makes up the information in the phone book.[101] According to Roos,[102] it is commonplace in the literature on data protection to use data and information interchangeably; the same is the case in this study.

Personal information is the set of all data that is associated with a specific individual, for example, date of birth, gender, home address, name of first pet, favourite chocolate, high school of graduation and other similar information. Personal information thus has meaning only through the ways in which it associates or differentiates an individual from others. For the purpose of this thesis "personal information" refers to any information relating to an identifiable individual because that is the definition used in data protection instruments such as the EU Directive.

3.5 Data protection / information privacy

Data protection refers to the legal protection given to an individual in respect of the processing of data concerning him or her by another person or institution. Neethling

---

99 Processing is defined as converting raw data to machine-readable form and its subsequent processing (as storing, updating, combining, rearranging, or printing out by a computer. See *Merriam Webster Dictionary* 2010.

100 *Encyclopaedia Britannica* 2010.

101 The information contained in a phonebook is mostly personal information. Personal information is information about an identifiable individual. According to Waldo *et al*, personally identifiable information refers to any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other personally identifiable information can easily be derived, including, but not limited to, name, address, phone number, fax number, e-mail address, financial profiles, Social Security number, and credit card information. This is the sense in which it is used in data protection laws. See Waldo, Lin and Millett (eds) *Engaging Privacy and Information Technology in a Digital Age* 39

102 See Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 18.

defines privacy as an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.[103] (Underlining supplied)

Information privacy provides individuals with certain rights over the collection, use and disclosure of their personal information. The two terms, data protection and information privacy, refer to the same privacy interest, namely a person's right of control over the storage and usage of data about him- or herself. The two terms are used interchangeably in this thesis.

3.6 Data processing, Trans-border Data Flow (TBDF)

The principal objective of data protection law is to regulate the use of personally identifiable data. The ability to access, acquire, collate and correlate diverse data into personally identifiable information constitutes data processing;[104] this has been greatly enhanced by computer technology. The enormous capacity of advanced computing technologies enable commercial enterprises to profile[105] large classes of

---

[103] Neethling, Potgieter and Visser *Neethling's Law of Personality* 270. See also *Bernstein v Bester N O* 1996 (2) SA 751 (SCA) 789. Arising from this definition, the South African Law Reform Commission has argued that the entrenchment of the right to privacy in section 14 of South Africa's Constitution now compels the government to initiate steps to protect neglected aspects of the right to privacy in South Africa, such as data privacy or the protection of personal information. This is because section 7(2) of the Constitution provides that the state must respect, protect, promote and fulfil the rights in the Bill of Rights. See South African Law Reform Commission *Privacy and Data Protection* par 2.1.24.

[104] See n 101.

[105] The Electronic Privacy Information Center (EPIC) defines profiling as follows:

> Profiling is the recording and classification of behaviors. This occurs through aggregating information from online and offline purchase data, supermarket savings cards, white pages, surveys, sweepstakes and contest entries, financial records, property records, U.S. Census records, motor vehicle data, automatic number information, credit card transactions, phone records (Customer Proprietary Network Information or "CPNI"), credit records, product warranty cards, the sale of magazine and catalog subscriptions, and public records. Companies collect information derived from a number of resources to build comprehensive profiles on individuals in order to sell products and to sell dossiers on behavior. This is often done without notice or extending a choice to the individual to opt-out of the dossier building.

See EPIC *Privacy and Consumer Profiling* [online].
Rosen also observed that "when intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences." See Rosen *The Unwanted*

individuals and the information gained thereby can be used to influence or alter the way people behave and thus become a means of social control.[106] Trans-border data flows (TBDF) refer to the exchange of personal information across national boundaries particularly through computer networks and telecommunication lines.[107]

4. RESEARCH METHOD

As pointed out above, there is a paucity of research on privacy in relation to the new technologies of the Information Age in Nigeria. The research shall therefore be relying greatly on material from outside the jurisdiction. The methodology will be descriptive, analytical, comparative and argumentative, depending on the dynamics of the various themes to be dealt with. The foundation upon which the research will draw consists of academic research and other writings on privacy and the impact of information and communication technologies (ICTs) in society; as well as studies of surveillance and of corporate and individual attitudes towards technology and privacy. Law books and journals (hardcopy and electronic), policy papers, government reports, NGO reports, laws, newspapers, websites and other published articles dealing with ICTs and their implications for privacy, will be primary sources. They will be particularly useful for some of the questions outlined in the research project.

The thesis will contend that a developing country like Nigeria at the nascent stage of technological development, need not deal with only infrastructural deficiencies, but also with deficiencies in the legal system. In dealing with the legal system, Nigeria must also look to those countries that have had good exposure to information technology practices and whose legal systems have developed sufficiently to address the legal issues arising from the use of these technologies. For this reason, this research will embody a comparative analysis of research studies and position papers with a legal or public-policy perspective on the development of privacy protection

Gaze: The Destruction of Privacy in America 9.

106 Flaherty *Protecting Privacy in Surveillance Societies* 9. Flaherty asserts that the uncontrolled acquisition of personal data can become a force determining behaviour by producing a "chilling effect" on personal behaviour.

107 See par 1.2 above.

laws and systems in a number of countries, particularly the UK, US, Australia and South Africa.

The UK is chosen because, like Nigeria, it is a common law country with EU Directive-compliant data protection law; the US because it presents an amalgam of privacy protection mechanisms, most notably the market regulated regime. Also, because of the constant flow of new technologies that impact privacy, America remains an active arena for the discussion of privacy issues. Australia has adopted a mixture of the EU and American systems and like Nigeria, is a common law country as well. In the case of South Africa, the Protection of Personal Information Act 4 of 2013 was signed into law by the President on 26th November 2013. The law will come into effect one year after the date of the President's assent. As one of the few countries in Africa to embark on a preliminary study of the issues relating to privacy prior to legislation, some of the views expressed in the study will be reviewed and assessed in relation to Nigeria. The research will draw upon other writings in fields removed from privacy and ICTs, because they will provide important analytical themes and interdisciplinary perspectives that the research will draw upon.

5. RESEARCH OUTLINE

Chapter 1 gives an overview of the research problem and outlines the parameters and contexts of the research study. Being an introductory chapter, it sets out the background information that will put the research problem in proper perspective. It also sets out the research framework or outline and the methodology that will be used in the research. Finally, it provides brief definitions of the key terms used in the body of the research.

Chapter 2 gives an overview of the convergence of information and communication technologies and their contributions to global commerce. The chapter is premised on the notion that technology has been at the heart of human progress since earliest times and technological advances have driven human development and interaction. It identifies some of the information and communication technologies that have had an impact on modern societies thereby giving rise to new ways of doing things. It traces the development of the Internet and its impact on commerce as well as some

of the issues relating to personal information privacy. The chapter also examines the global trade in information and the recognition of information as a commodity, information goods, trade in services and electronic commerce. Finally, it examines the nexus between globalisation, trans-border flows of information and the privacy concerns they raise.

Chapter 3 gives an introduction to the Nigerian state in the Information Age. The focus of the research being Nigeria, it examines whether the country is plugged into the Information Society and what the state of her infrastructural and regulatory capacities are. The phenomenal increase in telecommunications facilities and telephone density, coupled with the growing resort to online banking and other Internet-based commercial activities call to question the preparedness of the country's institutional and regulatory infrastructures to plug into the global networked economy and thus give Nigerians access to the Information Society. A critical assessment is made of the regulatory framework overseeing Nigeria's information and communications technology infrastructure and the privacy issues raised by the recent mandatory registration of mobile phone SIM cards in the country.

Chapter 4 explores the theoretical foundations of privacy and their perceptions in Western and African/Nigerian intellectual and cultural traditions. This chapter is pivotal in the examination of the issues raised in this research as it will analyse the basic premises of information privacy in the digital age and determine whether information privacy is dead as people like Scott McNealy of Sun Microsystems[108] would have us believe. His comment reflects what many people believe, namely that ICTs, in particular, computers and digital electronic networks, have dramatically and irrevocably diminished our privacy. The question that arises therefore is whether McNealy is right or not.

The chapter also examines the impact of technology on privacy and issues arising therefrom, such as interception of communications, surveillance, workplace monitoring, data retention, the ICT/Internet/ telecommunications interface and how

[108] The Chief Executive Officer of Sun Microsystems was reported to have told a group of reporters and analysts at an event to launch his company's new product, the Jini technology. See *Wired* "You have zero privacy anyway". [online]

they compromise information privacy in the collection, processing and disclosure of information. The impact of technology on the collection and processing of information is at the heart of the current heated privacy debate; this chapter examines the role technology plays in diminishing the privacy rights and interests of both users and non-users of the various technologies.

Chapter 5 explores how unbridled access to information and the global trade in information and information products affect information privacy. It traces the historical development of the use of technology in the collection of information and the commercial uses of personal information. It highlights the business models that utilise personal information in the new marketplace where information and information products are sold. It highlights the long-standing conflict between the right to privacy and right to information. The conflict between privacy and freedom of expression[109] is often resolved in favour of the latter on a presumption of primacy that is questionable and all the more aggravating in the face of advancing technologies aimed at circumventing the whole notion of privacy.

Chapter 6 examines the issues relating to the regulation of trans-border data flows (TBDF) and their implications for Nigeria. The focus is on the global regulatory framework for data protection. It examines the impact of the EU *Directive on Data Protection* and the restrictions it places on the collection and use of data, restrictions on data flows to countries outside the EU and the question of adequacy of protection. The chapter explores the evolution of trans-border data flows regulation and how the global flow of information threatens not only the privacy of personal information but also national sovereignty.

The chapter also explores the impact of globalisation on TBDF and the legal and jurisdictional issues arising from international data flows. It examines the reasons for regulating TBDF and the emergence of the data protection regime in response to the threats accompanying TBDF. Globalisation is often thought of in terms of the diffusion of goods, services and technologies across borders; the extra-territorial

---

[109] The right to freedom of expression includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

application of regulatory regimes is another major element of globalisation. The regulation of TBDF in one country or regional grouping of countries has a ripple effect in another country and raises questions about the sovereignty of nations in a globalised world. The chapter will examine this issue in the light of the extra-territorial reach of the EU Directive 95/46/EC.

Chapter 7 will focus on the imperatives of integration into the global network economy for sustainable growth and national development. As a developing country, Nigeria recognises the critical importance of the global market economy and the benefits that its empowering technologies such as the Internet and ICTs offer for national development. International trade is driving the diffusion of goods, services and technologies and consequently, global integration. Being an active member of the global network economy is essential to Nigeria's economic growth. The growth of trade in services in the global economy, coupled with the rising use of ICTs, provides developing countries like Nigeria new opportunities for integration into the global economy. Integration is however dictated by adherence to evolving regulatory regimes.

The chapter explores the challenges that confront Nigeria's desire to plug into the global economy and examines the links between trade, international standards and market access. It identifies regulatory standards as barriers to trade and integration; international regulatory frameworks have become technical and non-technical barriers that developing countries like Nigeria must overcome in order to integrate fully into the global network economy in the 21st century. Data protection legislation is both a barrier and gateway into the global network economy and the EU Directive on data protection has emerged as the global data protection standard. The threat, implicit in the Directive, to restrict trans-border flow of data to countries outside the EU who have inadequate data protection laws, gives the Directive its commanding position as a barrier/gateway to integration especially for developing countries.

One question the chapter will seek to answer is whether the EU Directive on data protection is a violation of WTO's trade rules and what Nigeria's response should be to the Directive. To answer the question, the EU's process of assessing adequacy of data protection in a third country will be examined. While arguing that law reform is an important and necessary vehicle for economic development and integration into the

global economy, the chapter will call for the development of a Nigerian data protection framework and proffer reasons why Nigeria should enact a data protection law.

Chapter 8 will explore the motivations and objectives that drive the enactment of data protection laws globally and how such motivations will play out in Nigeria. Perspectives from socio-cultural studies will be examined in order to explain why economic and not cultural motivations will power the drive to enact a data protection law for Nigeria. In arguing for the enactment of a data protection law for Nigeria, a comparative review of information privacy protection regimes in other countries will be undertaken with a view to aiding policy makers in choosing the right regulatory model of data protection for Nigeria. European and US approaches to data protection, as well as other common law countries like Australia and the UK will be examined. South Africa's data protection plans and how they might affect Nigeria will also be examined.

An overview of the main regulatory models will be presented with a highlight of the strengths and weaknesses of each model. Recognising also that regardless of the model that will be chosen, regulatory theory distinguishes between principles-based and rules-based regulation, the chapter will highlight the arguments for rules-based and principles based regulatory models in the light of Nigeria's peculiar socio-political environment. At the conclusion, useful recommendations will be made to assist Nigeria in addressing the privacy issues that will be highlighted in the course of this study.

CHAPTER 2

EMERGENCE OF THE INFORMATION ECONOMY: THE CONVERGENCE OF TECHNOLOGY, INFORMATION AND COMMERCE

1. INTRODUCTION: TECHNOLOGY AS CATALYST FOR HUMAN DEVELOPMENT

This chapter will explore the emergence of the information economy, its enabling technologies and their roles as catalysts for human development in modern societies. It will trace the development of the Internet and its impact on commerce and telecommunications as well as personal information privacy. The chapter will examine the global trade in information, the recognition of information as a commodity, information goods, trade in services and electronic commerce. It will be argued that the enhanced global trade in information as commodity and the rise of new business models specialising in the collection, processing, storage and sale of personal information, contributed significantly to the rise of trans-border data flows of information and the privacy concerns they raise.

Technology has been at the heart of human progress since earliest times,[110] and technological advances have always driven human interaction and commerce. The state of a given society's technological development always determined, from earliest times, the possibility and extent of that society's interaction with others, by providing the means to venture beyond its immediate environment.[111] The march of technological development and innovations has been greatly impacted by the

---

110 UNDP *Human Development Report 2001: Making New Technologies work for Human Development* 26.

111 The invention of the wheel in about 3500 B.C. marked the breakthrough in inventions that accelerated the spread of human civilisation intercourse. Other inventions such as boats, sailing ships represent great milestones in the march of modern civilisation. These early technological inventions truly determined the scope and extent of people to people interaction. See *The World Book Encyclopaedia* Vol 19 (2002) 385.

invention of paper and printing.

The Egyptians perfected the process of converting papyrus to a portable medium for inscribing or writing characters on.[112] The Chinese developed silk parchment and invented the earliest form of paper as we know it today, while the Arabs spread the use of paper to Europe and consequently to other parts of the world.[113] These innovations have signified important milestones in man's technological progression.

The introduction of paper into Europe in the 12th century ultimately led to the invention of printing in the 15th century.[114] The spread of printing in Europe revolutionised learning, which in turn has effectively brought man in terms of knowledge and information, to where we are today.[115] Some regard the invention of printing as one of the greatest innovations in history, because it ushered in a period of rapid expansion of knowledge and information not seen before then in the world.[116] The introduction of printing into Europe in the 15th century had the effect of multiplying the output of books while at the same time cutting the costs of production.[117] Printing made information available to a larger segment of the population who were eager for information of any variety.[118]

---

112 Papyrus is an early form of paper made from the stalks of the papyrus plant that was once abundant in the Nile Delta of Egypt. Papyrus is first known to have been used in Ancient Egypt. See *The World Book Encyclopaedia* Vol 15 (2002) 141.

113 Lucien and Martin *The Coming of the Book: The Impact of Printing 1450-1800* 30-32.

114 The use of paper was first introduced into Europe in Spain. See Lucien and Martin *The Coming of the Book: The Impact of Printing 1450-1800* (1976), for a historical account of the introduction of paper into Europe.

115 See Eisenstein *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe* 3. Johannes Gutenberg is traditionally considered the inventor of Western printing even though printing had been invented by the Chinese in 1045.

116 Printing was recognised as one of the inventions that changed the appearance and state of the whole world, the other two being gunpowder and the compass. See Francis Bacon *Novum Organum* 129, quoted in Eisenstein E *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe* (1980) 43. Eisenstein, while describing the consequences that ensued once printers had begun to ply their new trades throughout Europe, alludes to the invention of printing as a "communications revolution" (44).

117 *Encyclopaedia Britannica Student and Home Edition* (CD) "Printing".

118 Ibid.

1.1 The printing press - pioneer information and communication technology

Printing made the preservation and dissemination of knowledge possible and easier. Printing thus became the most important catalyst in the advance of science, technology and scholarship.[119] It is therefore arguable that the printing press initiated an "information revolution" much like what the Internet and the different information and communication technologies are doing today. The printing press was the first significant communication technology to have a global impact and was the foundation upon which great and revolutionary concepts and innovations were built. Like the printing press of earlier centuries, the telephone, radio, television, computer, fax and other communication technologies of the 20th century opened up communications, reduced isolation and enabled people to be better informed and to participate in decisions that affect their lives.[120]

As Alan Greenspan, a former Chairman of the Federal Reserve Board in the US said:

> The newest innovations, which we label information technologies, have begun to alter the manner in which we do business and create value, often in ways not readily foreseeable even five years ago.[121]

The words quoted above are as true today as they were in 1999 when they were first spoken. It is undeniable that the world is presently undergoing an unprecedented technological revolution. On a global scale, information and communications technologies are generating a new revolution that is already as significant and far-reaching as those of the past, such as the printing press, telephone, radio, and television. It is a revolution based on information, which has increased in leaps and bounds. This revolution now enables us to process, store, retrieve and communicate information in whatever form it may take - oral, written or visual - in ways never imagined before and unconstrained by distance, time and space.

---

119 See n 115. According to Eisenstein, the shift from manuscript to printing revolutionised all forms of learning.

120 See n 116.

121 Henry et al *Emerging Digital Economy* 1 [online].

It has always been the case that whenever new technological innovations were presented to the world, they have inevitably been accompanied by major and sometimes dramatic influences on the societies that embrace them. Such was the case with the steam engine that ushered in the Industrial Revolution by providing power that enabled a more efficient and large-scale production of goods.[122] Each subsequent technological innovation from then on, has contributed immensely to the growth of world civilization and economic development, particularly in those countries where machines such as trains, automobiles and airplanes, were first developed.

1.2 Newer information and communication technologies

The 20th Century is now gone, but it leaves in its wake some of the most outstanding inventions in the history of civilisation. Each new invention has had profound effects on world societies. Perhaps, the greatest of these inventions is the integrated circuit (IC) which was invented in 1959 by Robert Noyce and patented in 1961. This invention made it possible to put an entire electronic circuit on a tiny silicon chip.[123] The microchip or microprocessor has had the greatest impact, compared with other important milestone inventions such as the radio, telephone, television etcetera. These technologies now incorporate the microprocessor in their systems. Without it, none of the other great technological innovations would have been able to touch the lives of as many people as they do today. According to John Hollar, "It became the electronics technology through which we have created our contemporary digital world. It is indispensable to modern life."[124] The mass production of virtually all electronic gadgets in use today was made possible by the microchip and even more

---

122 James Watt, a Scottish inventor and mechanical engineer developed the steam engine improving on earlier designs by Thomas Savery and Thomas Newcomen. Their designs could only be used in the mining industry principally for pumping water. Watt's engine was capable of being used in many different industrial settings and without being located near to a water source. This freedom gave impetus to the Industrial Revolution by encouraging the spread of factories and thereby, mass-production of goods in diverse locations. See *The World Book Encyclopedia* Vol 21 (2002) 148.

123 See n 110 at 32.

124 See Ogg "Toasting the birthday of the integrated circuit" [online]. Hollar, the CEO of the Computer History Museum, made the statement at the 50th anniversary celebration of the invention of the integrated circuit, at the Computer History Museum, Mountain View, California, in 2009.

significantly, it brought the desktop computer to the reach of the individual user.[125]

The first high-speed electronic computer, ENIAC, (Electronic Numerical Integrator And Computer) was built in 1946 and signalled the start of the computer industry.[126] The early computers produced in the 1950s were massive mainframe juggernauts that would fill a whole room and were affordable to governments and large corporate entities only. The first commercial microprocessor was introduced into the market in 1971, while the first personal computer was produced in 1975, but it was not until 1981 that IBM, (International Business Machines) introduced the personal computer into the market on a commercial basis.[127] The personal computer, as the name suggests, brought computing to a personal level and sparked off the ICT revolution which is still impacting the whole world through a myriad of on-going technological innovations.

1.3 Convergence of technology, information and commerce

The most significant of these technological innovations in the last century was the convergence[128] of technologies in communication, computing (computers, software, services) and broadcasting (publishing, entertainment and information providers), to create the interactive multimedia and the information highway. This convergence of computing and communications technologies, which are now called Information and Communication Technologies (ICTs), heralded the Information Society of the late 20th century. The concept of the Information Society has taken centre stage in the 21st century public discourse, simply because the synergies produced by the convergence

---

125 See n 110.

126 *The World Book Encyclopedia* Vol 4 923.

127 Id at 924.

128 Convergence refers to the power of digital media to combine voice, video, data and text, in new applications, devices and networks. The EU Commission, in its *Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications of Regulation: Towards an Information Society Approach* COM (97) 623 final, 3 (1997) ii, recognises that convergence, pertaining to telecommunications, information technology and broadcasting, is occurring at the technological level such that digital technology now allows both traditional and new communication services whether voice, data, sound or picture, to be provided over many different networks. While acknowledging the lack of precise definition, it sees convergence most commonly expressed as:

- the ability of different network platforms to carry essentially similar kinds of services, or
- the coming together of consumer devices such as the telephone, television and personal computer.

of telecommunications and computer technologies continue to impact societies in ways never imagined. The *Bangemann Report* of 1994[129] helped to draw world attention to the opportunities afforded by the emerging information society powered by ICTs.

1.3.1 Information society

The *Bangemann Report* pointed to the fact that ICTs were generating a new industrial revolution based on information, with a huge capacity to change the way we work and live together. The information society was thus seen as capable of improving the quality of life of Europe's citizens, the efficiency of Europe's social and economic organisations and to reinforce cohesion. The vision of ICTs being deployed as potent agents for development has not only resonated in the Western developed societies, but increasingly so in the developing countries of Asia and Africa where ICTs are portrayed as providing opportunities to take giant leaps in the race towards development.

This view of ICTs transforming the industrial society into an information society was endorsed by the Organisation for Economic Cooperation and Development (OECD) as a public policy instrument in 1997 as a follow up to the *Bangemann Report*. Recognising that the development of a global information society can help governments contribute to further enhancement of public goals, the OECD declared that:

> The development of an information society is expected to have important beneficial impacts on economies and societies; it is expected to stimulate economic growth and productivity, create new economic activities and jobs. As well, a number of social benefits are expected to develop, including improved education opportunities, improved healthcare

[129] In December 1993, the European Council called for a report that would recommend specific measures to be taken into consideration by the Community and the Member States for the infrastructures in the sphere of information, to be prepared for its meeting that was to be held in June 1994. The Report titled, *Report on Europe and the Global Information Society: Recommendations of the High-level Group on the Information Society to the Corfu European Council. Bulletin of the European Union, (Bangemann Report) Supplement No. 2/94 (1994)*, was prepared by the High-Level Group on the Information Society chaired by Martin Bangemann. "On the basis of this report, the Council will adopt an operational programme defining precise procedures for action and the necessary means. This Report urges the European Union to put its faith in market mechanisms as the motive power to carry us into the Information Age." See n 1 at 4.

delivery and other social services, and improved access to cultural and leisure opportunities.[130]

The concept of the Information Society is grounded in the notion that the world is now faced with an inevitable and inexorable march of a technology-driven global networked society, which will be beneficial to all and bring about great improvements in all facets of national development.

The engine that drives this technology-based development comprises the vast technologies and applications that make up what is generally referred to as information and communication technologies.[131] They are seen as presenting developing countries with the means to speed up economic and social development. As a consequence, national development has in the last thirty years or more, witnessed a paradigm shift from the natural resource exploitation model of the last century. Development is now seen as knowledge-based and driven by information technology, while skills and knowledge are seen as the basis of comparative and competitive advantage, nationally and internationally.[132]

Central to this new model or concept of development are the twin resources of knowledge and information, because of their inherent capacities to enhance the process of problem solving. Development, as Okpaku argues, is "simply the process of problem solving or responding to new challenges with a view to mastering them."[133] Harnessing the potentials and capacities of knowledge and information for development has therefore become one of the most critical issues facing most developing countries today.

---

130 OECD *Global Information Infrastructure-Global Information Society (GII-GIS): Policy Requirements* 6. The aim of the report was "to develop recommendations for policies that fully exploit the contributions of advances in technology in the context of Global Information Infrastructures - Global Information Society (GII-GIS). This background report examines developments in GII-GIS and provides recommendations on policies." (5).

131 Castells *Information Technology, Globalization and Social Development* 4 [online].

132 Okpaku (ed) *Information and Communication Technologies for African Development: An Assessment of Progress and the Challenges Ahead* 22.

133 Ibid.

1.3.2 The digital divide

However, the spread of ICTs across the world has not been without its problems; the spread is not even,[134] nor equitable and has brought into sharp focus not only the glaring division of the digital world into the haves and have-nots,[135] but also new problems associated with the proper management and supervision of the deployment of these technologies. One of such problems is the conflict between the right to information and the right to withhold information, particularly personal information, recognised generally as the right to information privacy with which this work is concerned.

The overwhelming reliance on ICTs as tools for development in the last two decades has meant that any country that aspires to participate in and benefit from the several advantages of the Information Revolution, must invest heavily in the necessary technologies and personnel to run them. The capital-intensive nature of these technologies make them not easily affordable to many poor countries, particularly in Africa, thus the digital divide remains, either qualitatively or quantitatively.[136]

---

134 See n 131. According to Castells: "… information and communication technology is the essential tool for economic development and material well-being in our age; it conditions power, knowledge and creativity; it is, for the time being, unevenly distributed within countries and between countries; and it requires, for the full realization of its developmental value, an inter-related system of flexible organizations and information-oriented institutions."

135 The digital divide is a social/political issue referring to the socio-economic gap between communities that have access to computers and the Internet and those who do not. The term also refers to gaps that exist between groups regarding their ability to use ICTs effectively, due to differing levels of literacy and technical skills, as well as the gap between those groups that have access to quality, useful digital content and those that do not. With regard to the Internet, the access is only one aspect, but the quality of connection and auxiliary services, processing speed and other capabilities of the computer used, and other factors could also be part of the issue. According to the OECD,

> The digital divide reflects various differences among and within countries. The ability of individuals and businesses to take advantage of the Internet varies significantly across the OECD area as well as between OECD and non-member countries. Access to basic telecommunications infrastructures is fundamental to any consideration of the issue, as it precedes and is more widely available than access to and use of the Internet. See OECD *Understanding the Digital Divide* 1

136 See n 110 at 1-8.

2. THE INFORMATION ECONOMY

2.1 Emergence of the information economy

In the 1950s, economists began to recognize information as an important basis for competitive advantage in a country's economy. This period witnessed a shift from industrial mass production of goods to information processing activities that were powered by new ICTs. One of the earliest studies of the changing phenomenon was carried out by Fritz Machlup,[137] who found that, by 1959, workers in the US, whom he classified as being in "knowledge-producing occupations",[138] had surpassed those in other occupations in terms of their numbers. He used the term "knowledge-based industry" to describe the new emerging economy. Machlup distinguished between five sectors of the knowledge-based industry, namely education, research and development, mass media, information technologies and information services.

This emerging new economy was characterised by Daniel Bell[139] in 1976 as a "post-industrial society" in which services constitute the cornerstone of economic activities. According to Bell, "[a] post-industrial society is one in which the majority of those employed are not involved in the production of tangible goods."[140] Porat,[141] on the other hand, described the emerging sector of the US economy in the 1970s as the "information economy". According to Apte and Nath, Porat distinguished between two sectors of the economy: the "primary information sector" made up of industries producing information goods and services, and the "secondary information sector" made up of workers engaged in indirect information activities that are used as inputs in the production of other goods and services.[142]

The consensus among commentators is that a country with an information economy is one in which the society is organized in such a way that the generation, processing

---

137 Machlup *The Production and Distribution of Knowledge in the United States*.

138 Ibid at 44-50.

139 Bell D *The Coming of Post-Industrial Society* 348.

140 Ibid.

141 Porat *The Information Economy: Definition and Measurement*.

142 See Apte and Nath *Size, Structure and Growth of the US Information Technology* 6 [online].

and transmission of information are the fundamental sources of productive capacity and comparative advantage.[143] Information and the information technologies that empower information usage are recognised as essential tools for development; they are the tools that can empower the poor, enhance skills, increase productivity and improve governance at all levels.[144]

Manuel Castells[145] sees the availability and use of ICTs as a pre-requisite for economic and social development. He considers them to be the functional equivalent of electricity under the Industrial revolution. As Christine Qiang *et al*,[146] have observed, there is a growing consensus in the development community that in order to improve the investment climate in their countries, governments should place a high level of priority on improving access to information and communication technology (ICT) as well as its quality. They argue that enterprises that use ICT more intensely are more productive, grow faster, invest more and are more profitable.[147]

However, not all commentators share the same enthusiasm; Alice Rivlin for example, while agreeing that the IT revolution has had a significant impact on the economy of the US, points out that the greater share of economic production is still undertaken in the production and distribution of non-IT items such as food, clothing, home furnishings, cars, haircuts and medical care.[148]

For his part, Perelman[149] cautions that observers should not be carried away by their enthusiasm for the role of information. He agrees with Jussawalla[150] that the bulk of the estimates for the size of the information sector in the advanced capitalist

---

143 Machlup *The Production and Distribution of Knowledge in the United States* 44-50 and Bell *The Coming of Post-Industrial Society* 348.

144 See Schware "Overview: E-Development: From Excitement to Effectiveness" xiii.

145 See n 130 at 3.

146 Qiang, Clarke and Halewood "The Role of ICT in Doing Business" 57.

147 Id at 62.

148 Hakkio *Economic Policy for the Information Economy* 9 [online].

149 Perelman 1996 (2) *Mich Telecomm & Tech L Rev* 93.

150 Jussawalla *Information Economies and the Development of Pacific Countries* 15, 23-24.

countries runs from around 25 per cent to 40 per cent of the total economy. He also argues that some of the apparent growth of the information sector is an illusion because it is due to changes in the structure of the economy where, he asserts, virtually all work involves the processing of information.

While conceding that there is only little empirical evidence to show that informational activities have made significant impacts on the national economies of the most advanced countries, Cogburn and Adeya caution that "the lack of empirical evidence must not blind us to the transformative power of this new economic paradigm."[151] They assert that notwithstanding the debates on the information economy, one fact stands out clearly and it is that both information and knowledge are becoming fundamental components of socio-economic development. They observe that globally, investments in intangible goods and services are growing more rapidly than investment in physical goods and services and those nations which are endowed with greater information and knowledge resources are becoming more competitive.[152]

2.2 Technologies of communication and commerce

Modern technology is usually understood as referring to the combination of computers and communications devices which have in the last several decades changed the way we handle information. These changes are also impacting on national and international trade. Indeed, a major outcome of the convergence between computer and communication technologies is the growth in electronic commerce. Convergence is not just about technology; it is about services and about new ways of doing business and of interacting with society.[153] The global nature of communications platforms today, in particular the Internet, is providing the means to open the door to the further integration of the world economy.[154]

---

151 Cogburn and Adeya "Understanding Globalisation and the Information Economy" 4 [online].

152 Ibid.

153 EU Commission *Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications of Regulation- Towards an Information Society Approach* 1-3.

154 Ibid.

2.3 ICTs and international trade

One of the pillars of international trade is the services sector such as education, financial, health and telecommunication services.[155] In the past, a firm based in the US, for example, offering such services in Nigeria or another country, had to either be physically present in Nigeria or had to set up a local representative, usually a subsidiary, whose operations were subject to Nigeria's policies. With the convergence of computer, telecommunications and broadcasting, these services have a wider reach because they can be offered online.[156]

Electronic banking, online educational services, telemedicine and data processing are examples of core trade in services items governed by the World Trade Organisation's *General Agreement on Trade in Services* (GATS).[157] The electronic dispensation of such services is made possible by ICTs and increasingly they do not only constitute a significant volume of international trade, but also major sources of exports by leading industrial countries such as the US, Japan and Germany.[158]

The ability of any country to participate in the GATS-mediated trade in services is largely dependent on its level of ICT connectivity. A country that has poor ICT infrastructure cannot offer services such as online education, telemedicine and online banking, nor can it effectively participate in the New Economy that these technologies support. Furthermore, it is now not enough to simply provide the technology that assures connectivity, it is equally important to ensure that there is unimpeded free flow of information through the technologies.[159]

---

155 UNCTAD *The Tradability of Consulting Services and its Implications for Developing Countries* iii.

156 Id 2-3.

157 Braga 1996 (33) *Finance & Development* 34.

158 Mattoo and Wunsch *Preempting Protectionism in Services* 2-5 [online].

159 The OECD in its 1980 *Recommendation of the Council of the Organisation for Economic Cooperation and Development concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* recognised that:

> …although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information; that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices; that transborder flows of personal data contribute to economic and social development…

One of the ways to ensure this is by harmonising the national laws that regulate the flow of information across borders.[160] In addition, and bearing in mind the current low levels of ICT penetration in Nigeria, it is necessary that the use of ICTs be integrated into the educational system at all levels and businesses in the formal and informal sectors be encouraged to adopt the technologies having been made aware of the limitless opportunities for growth available through the use of ICTs. The educational system, having embraced ICT training in its curriculum, should then be able to provide trained personnel for the different sectors of the economy to drive the deployment and use of the technologies. ICTs comprise the telephone at the most basic level and satellite communications at the more advanced level. The Internet bridges the whole spectrum of the ICTs.

2.4 The technologies

2.4.1 Introduction

In the late nineteenth and early twentieth centuries, the foremost and perhaps most advanced means of communication was the telegram. The story of the telegram began in 1837 when Samuel Morse[161] operated the first telegraphic transmission. Prior to the invention of the telegram, there was a progression from human couriers to the postal service, which is still very much in use today. Early primitive societies used couriers to move messages and information within their settlement or across borders to other settlements. In a typical Nigerian village in the early part of the 20th century, the town crier was the official disseminator of public and private information. It is still possible today to see the last vestiges of this very basic communication network in some rural villages in Nigeria and presumably, also in other African nations, but their days are certainly numbered.

Over a period of time as societies became more settled, centralised administrations were put in place and the human couriers gave way to government run postal services. Commercial activities and contractual relations were carried out and

---

160 See n 158 above. A good example of the efforts to harmonise cross-border laws is the *EU Directive 95/46/EC* See Michael *Privacy and Human Rights* 33.

161 *Encyclopaedia Britannica* "Telegraph" 2010.

created through the aid of hand-written letters. Inevitably, the law was called upon to resolve conflicts arising out of such personal or contractual relations created through the post. The modern law of contract is still regulated by rules and regulations fashioned in a time when commercial activities were undertaken in an age of relatively low-key technological advancements. For example, the 'postal rule' relating to acceptance of an offer communicated through the post evolved over the years through judicial law-making in England in the nineteenth Century.[162] After the novelty of postal service and its impact on business and personal relations had received the judicial stamp of approval, another technological breakthrough in communication came on the scene.

2.4.1.1 Telegram

The invention of the Morse code by Samuel B. Morse in 1835[163] introduced the telegram as a quicker means of communication. The obvious advantage of a telegram over a letter sent by post was that it was faster and facilitated communication by making it possible to send messages to those places where postal services could not reach. As inevitably happens with new inventions and their impact on human relations, the telegram created a few conflicts in the market place. The law, particularly common law, is slow to change unless something stirs it into action. It did not take a long time before the validity of the telegram, as well as the use thereof to create binding legal relations, were scrutinised by a court.

It appears the earliest judicial pronouncement on the validity of a telegram as a means of conducting binding business transactions, was the American case of *Durkee v Vermont* in 1856.[164] The Vermont Supreme Court held that the telegram was a proper proof of an original statement. Judicial pronouncements in later cases and in different jurisdictions have confirmed the validity of the telegram as a means

---

162 "The rule, put simply, states that an acceptance is effective once it is posted, rather than when it is actually received. The essence is that the acceptor has entrusted his communication to a third party or put the communication beyond his control." See Edwards and Waeld (ed) *Law & The Internet: Regulating Cyberspace* 98.

163 See n 161. The Morse Code was invented in 1835 but the first telegraphic transmission using the code was in 1837.

164 *Durkee v Vermont C Ry* 29 Vt 127 (1856). See also *Trevor v Wood* 36 NY 307, 93 Am Dec 262 (1867).

of communication.[165]

2.4.1.2 Telex

The telex is an international telegraphic message transfer service made up of a network of tele-printers. It originated in the UK in the 1930s and from there spread to the rest of the world.[166] Actually, it is the telegraph that evolved into the telex system in which machines eliminated the need for coding and decoding the messages. Users can type a message on one telex machine and the identical message would appear on the recipient's machine carried over telegraph and telephone lines. The telex also has received several judicial stamps of approval, for example, in the case of *Entores Ltd v Miles Far East Corporation*[167] the court had to decide when a contract is formed where a telex is involved. The court held that it is formed when the acceptance telex is received.

2.4.1.3 Telephone

Alexander Graham Bell invented the telephone in 1876 barely 18 years after the introduction of the telegraph.[168] It was meant to be an improvement on the telegraph; Bell's patent was titled "Improvement in Telegraphy".[169] His device was designed to transmit human voice over waves instead of electrical clicks like the telegraph. One fundamental difference between the two devices is the fact that while the telegraphic message is recorded in a more or less permanent form on the telegraph sheet, the telephone conversation, though instantaneous and therefore faster than the former, did not leave a record of what was discussed on the phone. This shortcoming accounted for an initial resistance to the telephone by some conservative businessmen who feared that such a medium without the capacity to

---

165 *Steven Jaques & Co v Mclean* (1880) 5 QBD 346.

166 See Beauchamp K *History of Telegraphy* 399.

167 (1955) 2 All ER 493; see also *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* (1982) 1 All ER 293.

168 Casson *The History of the Telephone* 1-12.

169 Ibid.

keep a record of transactions conducted through it, would be a dangerous device to toy with.[170]

However, the efficiency and versatility of the telephone was in the end enough to win over the most conservative businessmen. The telephone has become the most prevalent means of communication worldwide. Today, the telephone is a basic prerequisite for any business undertaking and it is the bedrock on which the fax and email capabilities in the business world are built.

2.4.1.4 The fax machine

A fax machine[171] is used in a facsimile transmission. This is a cheaper and easier way to transmit text and graphics over distances, by means of wire or radio waves. The machines are designed to scan printed text and graphic material before transmitting them through the telephone network to similar machines at the receiving end, where the documents are reproduced as near to the original as possible. Because of their low cost, reliability, speed and simplicity of use, fax machines have made a great impact on business and have revolutionised the way in which business is conducted today.

2.4.1.5 Electronic mail

The e-mail[172] is now the most popular component of the computer/Internet interface. It is a method of transmitting data, whether text or graphic files quickly from one computer to another over a network. The use of e-mail became widespread in the last decade and it has become a major communication tool in business and personal relationships. E-mail users send and receive messages from individual personal computers through the use of e-mail programmes.[173] It is in fact now possible to send

---

170 See n 168 at 16-19.

171 *Encyclopaedia Britannica* "Fax" 2010.

172 In 1971, Ray Tomlinson of BBN invented the e-mail programme to send messages across a distributed network. The original program was derived from two others: an intra-machine e-mail program (SENDMSG) and an experimental file transfer program (CPYNET). In 1972, Tomlinson modified the e-mail program for ARPANET where it became a quick hit. The @ sign was chosen from the punctuation keys on Tomlinson's Model 33 Teletype for its "at" meaning. See Zakon *Hobbes Internet Timeline 10.2* [online].

173 Examples of e-mail programmes include Microsoft Outlook, Outlook Express and Eudora.

faxes by e-mail and text messages to mobile or cell-phones through the short message service (SMS) which underscores the versatility of this tool of communication. To say that e-mail has had a profound impact on the world at large is to state the obvious. It has become virtually the single most important means of communication in the world today; previous methods of transmitting information such as regular mail, or 'snail mail' as it is now derisively called, telephone, courier, fax, television and radio have been largely eclipsed by e-mail. In the case of the new frontier of commercialism, electronic commerce (or e-commerce), e-mail is the preferred means of communication. It is easy to understand why this is so: the paperless nature of e-mail communication translates into corporate productivity and profitability by reducing operating costs and time usually spent on conventional paper-based communication.[174]

All the technologies discussed above have one thing in common; they are all used in the transmission of personal and business information and are implicated in trans-border data flows. A country's ability to integrate into the global network economy and participate meaningfully in that system is largely dependent on the country's level of ICT penetration and connectivity. The greater the country's level of ICT infrastructures, the greater its capacity to participate in trans-border flow of data. The country must also be able to regulate the flows of data in and out of its borders aided by these technologies. For Nigeria, the question is whether the country should wait until it attains a critical mass in ICT penetration (bearing in mind the current low levels) before harmonising its laws and regulatory regimes for secure trans-border data flows, or do so now, with the expectation that the penetration of ICTs will continue to rise. For reasons that would be elaborated in chapters 7 and 8, it is the view of this writer that the time to harmonise the regulatory regime with global standards is now.

[174] Gindin *Guide to E-mail and The Internet in the Workplace* [online].

3. ICTs AND THE INTERNET: THEIR IMPACT ON GLOBAL COMMERCE AND TELECOMMUNICATIONS

3.1 Evolution of the Internet

The Internet is the result of research and development collaboration between the military, defence contractors and the academic community involved in defence research for the US military in 1969 under the aegis of the Advanced Research Project Agency (ARPA).[175] It was developed as a basic network to connect the tripartite groups engaged in military research activities. The goal was to create a network of computers for which there would be no central operating computer, in order to reduce the risk of vital information and communication being lost if a computer on the network was damaged or compromised. This was of course the "cold war" era and the fear of the Soviet communists was the catalyst for technological innovation.

The term 'internet' is used to identify any collection of networks forming either a larger Local Area Network (LAN) or Wide Area Network (WAN) commonly called "intranets". The "Internet"[176], however, refers to the interconnected network of networks spanning the globe. Millions of individual computers are connected one to another, but each one is independently controlled by its owner who has agreed to use a common communication standard known as TCP/IP.[177] This standard, or protocol as it is called in the industry, makes it possible for different computers running on different operating systems to communicate with one another and share data, even though they may be hundreds of miles apart and have no direct connection to another. This standard communication protocol was deployed between 1973 and

---

175 In 1957, the then USSR launched Sputnik, the first artificial earth satellite. In response, the US in the following year set up the Advanced Research Projects Agency (ARPA). ARPA was set up in the Department of Defense (DoD) with the aim to establish US supremacy in the use of science and technology by the military. See *Encyclopaedia Britannica* "Defense Advanced Research Projects Agency (DARPA)" (2010). See also Leiner, Cerf, Clark *Brief History of the Internet* [online] for a definitive perspective on the history of the Internet by some of the key players in the development of the Internet, published by the Internet Society.

176 The term "Internet" was first used in a research paper written by Vinton Cerf and Robert Kahn in 1974. It described a "network of networks" that would link together computers across the country, and eventually the world. See Samuelson and Varian *The "New Economy"* [online].

177 Leiner, Cerf, Clark *et al Brief History of the Internet* [online]. In 1974 Vint Cerf and Bob Kahn published "A Protocol for Packet Network Interconnection" which specified in detail the design of a Transmission Control Program (TCP) and in 1978 the TCP protocol was split into TCP and Internet Protocol (IP).

1974.[178]

It is the TCP/IP standards that make the Internet possible. The most important feature of the protocol is that it defines a "packet switching" network; a method by which data can be broken up into standardised packets which are then routed to their destination through an indeterminate number of intermediaries.[179] This means that two different computers do not need to be in direct contact with one another in order to communicate. After the networking protocols were put in place, the Internet began to grow and expand as the necessary software and services that make up the Internet began to appear.[180]

Throughout this period, the original network, ARPANET, acted as the 'backbone' of the global Internet network. The fundamental objective for both ARPANET and the Internet was to create an enabling environment for resource sharing. This object continues to motivate the Internet today, although it is becoming increasingly commercialised. Since the 1980s, the Internet has been developing beyond its primary research roots to include both a broad user community and increased commercial activity. In 1991, the American National Science Foundation (NSF), which was then the Internet backbone administrator for the universities and research institutions, lifted restrictions on the commercial use of the Internet.[181] The Internet has been used for commercial purposes since then and the commercial sector is now by far the most rapidly growing sector of the Internet.[182]

---

178 Ibid.

179 See n 177 at 6-8. See also Basu *Global Perspectives on E-Commerce Taxation Law* 7-9.

180 Ibid. Some of the more well-known services on the Internet are:

- Gopher is a network protocol tool designed for search, retrieval and sharing of documents over the Internet, much like the World Wide Web.
- FTP is a File Transfer Protocol that allows users to copy files between their local system and any system they are connected to on the network.
- USENET is a worldwide network of public discussion forums accessed over the Internet. Millions of people scattered all over the world, make up the different discussion groups dealing with diverse issues. It is also a rich source of news and stories of interest to the members.
- World Wide Web ("WWW") is a service that operates over the Internet, by which people can read and write via computers connected to the Internet.

181 See Abbate *Inventing the Internet* 182. See also Catlett "Internet Evolution and Future Directions".

182 See n 177 at 12.

The invention of the World Wide Web in 1989 by Tim Berners-Lee and its deployment on the Internet greatly expanded the scope of the Internet, by adding to it on a continuous basis new communities of networks.[183] The Web, as it is commonly called in the IT industry, is a hypertext-based information service providing access to multimedia documents and databases. It is accessed through a browser such as Microsoft's Internet Explorer, Netscape's Navigator or Mozilla Firefox. It is one of the most effective methods of providing information to the widest audience possible. It has also levelled the playing field to some extent for small and big businesses that can project themselves to a global market place by publishing information about their goods and services on a web site.

3.2 Impact on global commerce

The Internet has opened up new opportunities for businesses to trade, advertise and operate across frontiers, and over borders. For businesses, large and small alike, the Internet and its varied technologies has become a window of opportunity to access a global marketplace.[184] What started out as a research and development endeavour has now become the backbone of a new way of doing business, namely electronic commerce. The potential of this is limitless.

The phenomenal rate of technological advances has resulted in the lowering of prices and an increase in the quality of goods and services. Consumers worldwide have come to identify successful enterprises as those who can deliver on lower prices and higher quality goods and services. These demands, combined with a globally competitive marketplace, have placed great pressures on the producers of goods and services to effectively use cutting edge technology to ensure they remain in business.[185]

---

183 See n 172. According to Zakon, the World-Wide Web (WWW) was released by CERN in 1991. The first Web server, nxoc01.cern.ch, was launched in Nov 1990 but later renamed info.cern.ch.

184 The logic of not re-inventing the wheel makes the Internet a good platform for businesses and researchers to share ideas and move forward. See Greenstein "Commercialization of the Internet" 151 [online].

185 Id at 154. According to Greenstein, the commercialisation of the Internet by the NSF at the same time as the introduction of the World Wide Web gave industry access to a new technological opportunity that thrived under a market- oriented and decentralised decision-making environment.

By means of the Internet, businesses are able to find suppliers and buyers, conduct valuable market research and publish information about themselves, their goods and services. The Internet helps businesses and all other interested users by providing free expert advice and presents opportunities for recruitment of new employees and access to information.[186] Accessing information on the Internet is faster than using conventional methods such as bulky business directories, thanks to ever improving search engines. The Internet also has unsurpassed capacity for the wide-scale dissemination of information; it allows for rapid communication by means of electronic mail and for cost-effective document transfer without the risk of damage or loss. It also enables peer communication between researchers and businesses.

One significant consequence of the impact of the Internet and its enabling technologies on global commerce is that it has opened new opportunities for developing countries to participate in global commerce. This in turn has led to increased trans-border data flows between countries and drawn attention to the issue of data protection. The following paragraphs and chapters will explore the opportunities and challenges that the Internet and its enabling technologies present to a developing country like Nigeria, to connect to the global network economy and how it should respond to the said opportunities and challenges.

3.3 The Internet and developing economies

The Internet offers entrepreneurs new business opportunities at low entry cost. This is particularly beneficial to businesses in developing countries that can take advantage of the opportunities offered by the Internet. For a modest investment, entrepreneurs can put themselves in a marketplace of millions of potential buyers.[187]

For less developed countries like Nigeria, the Internet provides unique opportunities to greatly expand their markets both externally and internally. Externally, the

---

186 Ibid.

187 According to a UNESCO Report, data exchange on the Internet is distributed as follows: 60 per cent for trade, 27 per cent for research, 9 per cent for administration and less than 5 per cent for education. The corporate sector is making increasing use of the Internet to penetrate markets around the world and for interchange with customers. The Report estimated that trade activities could generate revenue of between $7 billion and $40 billion in the year 2000. See UNESCO *World Communication Report: The Media and the Challenges of the New Technologies* 47.

Internet and other technologies may allow for low cost international trade by creating a level playing field for small, local businesses who want to engage in international trade alongside the big players; something which otherwise may not have been possible.[188] Internally, it can provide these same small-scale businesses, as well as the large ones, opportunities to expand their market exposure and give them access to a near limitless pool of resources in terms of information, communication and advertisement.

The Internet provides potentially the biggest marketplace in the history of commerce.[189] Furthermore, the World Wide Web, the most significant component of the Internet, has radically changed the dynamics and indeed the economics of information publication by allowing everyone to be a publisher with worldwide reach. The seemingly inexhaustible variety of documents, opinions, articles and works of all sorts on the Web demonstrate that millions of people worldwide are making use of its capability to disseminate information. But, as Cate notes, the Internet is only one tangible example of the explosion of digital information that includes other national and global networks, corporate computer and telecommunication systems, bulletin boards, nationwide paging services and countless other technologies.[190]

---

188 UNCTAD *The E-Commerce and Development Report* xvii, shows there is growing agreement about the positive contribution of ICT to productivity growth. Through the application of ICT, firms will become more competitive, new markets will be accessed and new employment opportunities created. All of these will result in the generation of wealth and sustainable economic growth.

189 Id at xviii. According to the report, the global number of Internet users continues to grow; the estimated number of users reached 591 million people in 2002. In a report published in October 2010, the International Telecommunications Union (ITU) estimated that by the end of 2010, the number of Internet users worldwide will surpass the two billion mark of which 1.2 billion will be in developing countries. See ITU *The World in 2010: ICT Facts and Figures* 4.

190 Cate *Privacy in the Information Age* 7.

4. THE GLOBAL TRADE IN INFORMATION AND INFORMATION PRODUCTS

4.1 Introduction: Information as commodity

With the rapid advancement in scientific and technological knowledge in the last two decades, particularly in ICTs, information has become the most critical element in global competitive advantage.[191] The OECD, in a 2005 report on employment, productivity and innovation, stated that the production of information goods and services accounted for over 70% of wealth and job creation in most of the advanced economies.[192] This has given information the character of a commodity in its own right. The concentration of economic activities around information and ICTs is now touted as the new basis of competitive advantage. According to Blumenthal, "[i]nformation has become the key to modern economic activity—a basic resource as important today as capital, land and labor [was] in the past."[193] Wilson and Al-Muhanna,[194] have noted that the exchange of information is now viewed as a part of the service sector of the economy.[195]

According to Sauvant[196], recent technological developments have led to increased use and application of automated information and the emergence of an international data market. He asserts that trade in information goods and services have increased considerably over the past decade, due in part to the growing trade in services. It was for this reason that the US took the position in the 1980s in favour of the inclusion of trade in services (of which trade data and data services constitute a significant component) on the agenda of negotiations on the *General Agreement on Tariffs and Trade*.[197]

---

191 Kranzberg "The Information Age: Evolution or Revolution?" 35-53.

192 OECD Report *Growth in Services: Fostering Employment, Productivity and Innovation* 2.

193 Ibid.

194 Wilson and Al-Muhanna" 1985 (22) No 4 *JPR* 291.

195 The services sector was not considered as trade until the early 1970s, when chapter 12, subchapter VI of the US Trade Act of 1974 defined "trade" for the first time as the exchange of services as well as goods.

196 Sauvant 1983 (37) *International Organisation* 359.

197 Brock (Foreword) to Feketekuty *International Trade in Services: An Overview and Blueprint for Negotiations.*

4.1.1 Information goods

Information good is defined very broadly as "anything that can be digitized – encoded as a stream of bits".[198] According to Nimmer and Krauthaus, an "information good" is by definition intangible and immaterial.[199] They assert that although such information goods may be recorded in an object or on paper, the tangible embodiment is not the information itself, nor does it determine who knows or can use it. For this reason, thousands of people can "possess" one piece of information at the same time. Unlike physical goods, they maintain, information can be used without being used up and can be sold without being given up.[200] One can sell and "deliver" information to another but still retain the information in his or her possession and for his or her own personal use.

4.1.2 Trade in services

Two decades ago, a large segment of economic activities constituting what was, and still is, generally referred to as the services sector of the economy, was not considered to be part of international trade. Services such as hotels, restaurants, health, education, insurance as well as transportation and communication were considered as components of the domestic market and therefore not open to international trade which was then dominated by merchandise goods.

Today, however, the situation has changed; the services sector is now considered a significant component of international trade. In the last decade, this sector has been one of the fastest growing in international trade. Hufbauer and Warren[201] define a service as "…an economic activity that adds value either directly to another economic unit or to a good belonging to another economic unit." According to Mattoo,[202] the main reasons that account for the tremendous growth of trade in services are

---

198 Shapiro and Varian *Information Rules: A Strategic Guide to the Network Economy* 3.

199 See Nimmer and Krauthaus *Law & Contemp Probs* 1992 (55) No 3 105.

200 Ibid.

201 Hufbauer and Warren *Globalisation of Services* [online].

202 Mattoo *Economics and Law of Trade in Services* 1 [online].

technological progress, especially in telecommunications and information technology. Also contributing to the growth, are the broad trend towards liberalisation or regulatory reform in key service industries such as telecommunications and the adoption of privatisation and competition principles in many countries.[203]

Feketekuty[204] asserts that the information revolution has fundamentally changed the scope, character, and significance of trade in services. He argues that international trade in services has become an important issue, firstly because international trade in services has become big business and the enterprises that conduct this trade are counted among some of the largest corporations in the world. Secondly, it has become important because internationally traded business services are an increasingly strategic resource in the production of both goods and services. Furthermore, Feketekuty argues, the production of services based on the creation or processing of information, now benefits from the same kind of international specialization that led to the rapid growth of trade in goods in the past. Continuous innovations and adaptations of modern technology in the production and exchange of information goods and services are able to give countries the greatest competitive advantages in international trade and promote economic growth.[205] Globalisation is helping to integrate international markets for such goods and services.[206]

Trade in services is largely carried out by means of electronic commerce (e-commerce); service providers in industries such as finance, entertainment and communications deal primarily with information which is well suited to e-commerce.[207]

---

203 Ibid.

204 Feketekuty *International Trade in Services: An Overview and Blueprint for Negotiations* chp 3.

205 Rosenberg *A Background Review of the Relationships between Technological Innovation and the Economy* 18-48.

206 Blumenthal 1988 (66) No 3 *Foreign Affairs* 534.

207 There are services that require the proximity of the service provider, such as construction services, or the proximity of the consumer, such as tourism.

4.2 Electronic commerce

The defining characteristic of electronic commerce is the transaction of business through the electronic medium over computer networks. However, electronic commerce as a concept or mode of business transaction is not new. Prior to the current widespread use of the Internet as the medium of electronic commerce, a good deal of transactions involving the transfer of huge sums of money by means of electronic networks was regularly made.

Known generally as Electronic Data Interchange (EDI), such transactions were, and still are, widely used by banks and financial services companies, manufacturing firms, supplies and service companies.[208] They all rely on secure private electronic networks. In its most basic form, EDI simply transfers information between a series of interconnected computers; for example, a purchasing company's computer senses that its inventory levels are low, it initiates a sales transaction with the seller's computer using a proprietary agreed upon purchase order. Upon receiving the confirmation of an order from the purchaser's computer, the vendor's computer directs the shipping department to send the requested goods to the purchaser and it does this by using an agreed-upon format. This series of transactions is concluded without any human intervention.[209]

EDI may now be overshadowed by the Internet and its enabling technologies, but it is not exactly obsolete as it continues to be employed by several diverse companies to transact their businesses. The major limitation in respect of EDI compared with the Internet, is the fact that EDI enables only B2B (business-to-business) transactions whereas the Internet enables in addition, B2C (business-to-consumers), B2G (business-to-government) and G2C (government-to consumers) and C2C (consumer-to-consumer) transactions.

The phenomenal rise of the Internet in the last decade and the fact that it continues

---

[208] One example of EDI deployment in the financial services industry is the Society of Worldwide Interbank Financial Telecommunication (SWIFT) which was formed in 1973 and has its headquarters in Brussels. SWIFT operates a worldwide financial messaging network which exchanges messages between banks and financial institutions by means of electronic data interchanges through the SWIFTNet Network. See Baker and Byler 1983 (17) 5 *JWT* 458.

[209] Mckeon 1994 (7) No 4 *J Marshall J Computer & Info L* 511.

to expand its frontiers means that a wider spectrum of businesses and parties has been added to the commerce bandwagon than hitherto possible with EDI. Whereas under EDI, the most common type of transaction was the procurement of parts and financial services, today's e-commerce using the Internet platform encompasses, but is not limited to, database management and analysis, online computing services, Internet shopping, auction sales, Internet banking and brokerage, insurance services, education, entertainment, advertising, travel bookings and other emerging services.

Whatever the advantages of EDI and the Internet respectively may be, the truth is that both are essentially two sides of the same coin. The World Trade Organisation (WTO)[210] defines e-commerce as the production, distribution, marketing, sale or delivery of goods and services by electronic means. Electronic commerce is primarily an Internet application; it relies on the infrastructure of the Internet, which in turn, relies on a mixture of ICTs to operate. Catherine Mann[211] argues that the Internet and e-commerce integrate both services and goods sectors of a nation's economy across domestic and international boundaries through key synergies existing between telecommunications, financial services infrastructure, distribution, delivery and governance. The Internet and e-commerce both depend on and facilitate liberalization in these areas. She further asserts that:

> Electronic commerce and the Internet represent the opportunity to leap forward to the next stage of economic development, where value is created not just by resource endowments or manufacturing might, but also by knowledge, information, and the use of technology.[212]

The question, whether poor countries should spend their meager resources on ICTs and the Internet, has continued to generate a robust debate. Developing countries appreciate the need to get connected. However, the effects of poverty, combined with poor policy decisions, make the transition to e-commerce a rather daunting task for them. Countries that do not or cannot acquire the necessary technologies will be

---

210 WTO General Council *Work Programme on Electronic Commerce* WT/L/274 (1998).

211 Mann *Electronic Commerce in Developing Countries* 14 [online].

212 Ibid.

disconnected from the global network economy.[213] Indeed Mansell and Wehn have argued that "[c]ountries that do not implement electronic business networks will almost certainly find themselves disadvantaged in the conduct of trade and in their financial affairs."[214]

5. GLOBALISATION, TRANS-BORDER FLOWS OF INFORMATION AND PRIVACY CONCERNS

5.1 Globalisation: economic and political perspectives

Globalisation is one of those pervasive and diffuse phenomena that are hard to define. David Held *et al*[215] define globalization as:

> A set of processes, which embodies a transformation in the spatial organization of social relations and transactions – assessed in terms of their extensity, intensity, velocity and impact – generating transcontinental or interregional flows and networks of activity, interaction and the exercise of power.[216]

Economists see globalisation in terms of increased economic interdependence and the integration of all national economies into one global economy within the framework of a capitalist market.[217] Economic globalisation is manifested primarily in the multinational corporations (MNCs) that have greatly accelerated integration of the global economy, and in the growth of Foreign Direct Investment (FDI) and

---

213 Mansell and Wehn *Knowledge Societies: Information Technology for Sustainable Development* 214.

214 Ibid.

215 Held, McGrew, Goldblatt and Perraton *Global Transformations: Politics, Economics and Culture* 16. However, globalisation is essentially a contested concept. Its "contested" nature is evident in the ongoing debate about its meaning and nature. This debate has pitted "hyperglobalist," "skeptical," and "transformationalist" accounts of globalization against one another.

216 The flows referred to in their definition relate to the movements of physical artefacts, people, symbols, tokens and information across space and time, while networks refer to regularized or patterned interactions between independent agents, nodes of activity, or sites of power. Elsewhere, Held and McGrew observe that "[v]irtually all nation-states become part of a larger pattern of global transformations and global flows. Goods, capital, people, knowledge, communications and weapons, as well as crime, pollutants, fashions and beliefs, rapidly move across territorial boundaries. It has become a fully interconnected global order…" see Held and McGrew 1998 (24) *Rev Int'l Stud* 230.

217 Rajaee *Globalisation on Trial: The Human Condition and Information Civilization* 24.

corporate mergers and alliances in the 1980s and 1990s.[218] The growth in FDI emphasizes the role of the MNCs in the global economy. As suggested by Susan Strange, globalisation increases the power of the MNCs and will finally shift power from states to firms.[219]

Another dimension of the globalisation debate is the political perspective which also tends to emphasize the near impotence of the state in the era of globalisation.[220] The political perspective of the globalization debate argues that states are increasingly losing their capacity to govern, and to regulate the internal dynamics of the state in an increasingly borderless world. Appadurai in fact argues that "... the nation-state, as a complex modern political form, is on its last legs."[221]

"Non-state actors" such as MNCs, international governmental organizations (IGOs), non-governmental organizations (NGOs) and ethnic groups influence the state's authority in a situation of complex interdependence.[222] The emergence of regional and global law (also described as global humanitarian law) in the present era of

---

218 Sorenson 1998 (24) No 5 *Rev Int'l Stud* 83-100.

219 Strange *The Retreat of the State: The Diffusion of Power in The World Economy* 45. However, not all commentators on globalisation accept this conclusion; Hirst and Thompson for example, argue that there is no strong tendency toward a globalised economy and that the major advanced nations continue to be dominant. They offer three reasons for their arguments against the prevalence of economic globalization:

- that the current state of international interconnectedness is not unprecedented and that previous episodes of integration have generated a backlash and have ended in the regression of international trade and investment,
- that nation-states are not being overwhelmed and that the future of extended multilateral governance does not look promising — in a turbulent physical and international environment the nation-state may become more salient as a means of protection against global forces beyond supranational governance, and
- that there may be inherent limits to the growth of international trade, that borders do matter and that we may be approaching those limits.

See Hirst and Thompson 2002 *Cooperation and Conflict* (37) No 3 263.

220 Political globalisation is said to be "the shifting reach of political power, authority and forms of rule" wherein, political relations become closely and deeply linked, presenting a challenge to domestic/international distinctions of politics. See n 216 at 219-245.

221 See Appadurai *Modernity at Large: Cultural Dimensions of Globalization* 19. See also Rosenau *Turbulence in World Politics: A Theory of Change and Continuity*; Wriston *Foreign Affairs* 1997 (76) No 5 1972–1982, for similar views about the impact of globalisation on sovereignty.

222 Keohane and Nye *Power and Interdependence* 4. Although Keohane and Nye criticised modernist writers who "see our era as one in which the territorial state, which has been dominant in world politics for the four centuries since feudal times ended … is being eclipsed by non-state actors such as multinational corporations, transnational social movements and international organisations" (p 3), they pointed to the importance of "today's multidimensional economic, social and ecological interdependence" (p 4).

global politics, also challenges state sovereignty.[223] Consequently, one of the most important issues in the globalisation debate is the question of national sovereignty as it relates to economic, social and political processes. Economic activity is both national and international, and the state still mediates between them.[224] Nevertheless, as noted by Jayasuriya:[225] "Globalisation is reshaping the fixed and firm boundary between domestic and international spheres and changing our conception of the proper domain of domestic and international politics and law."[226]

One of the fallouts of modern globalisation is increased collection and dissemination of personal information about the users of the Internet and other tools of economic activity. Personal information now routinely flows across national boundaries seemingly without hindrance.[227] What makes the collection of information so attractive is the fact that:

> Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries.[228]

The economic value of personal data motivates firms to collect and process these data, by generating profiles of user behaviour for internal marketing purposes or for sale to other firms wanting customers of that type. Kling and Allen assert that the exchange of information dominates the contemporary market place, because of the expansion and use of computer technologies for large-scale record keeping and this has given rise to what they term "information entrepreneurialism".[229] It is now very

---

223 See n 216 at 219-243.

224 Ho Nov 12 2000 *The Sunday Times* (Singapore) 47.

225 Jayasuriya 1999 (6) No 2 *Ind J Global Legal Stud* 425.

226 Id at 447. Jayasuriya explains that the reconstitution of sovereignty represents the nationalisation of international law. He concludes that what this signifies is that the operation of the global economy requires extensive regulatory changes at the national level.

227 Bennett "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" 103.

228 Statement of Louis Joinet, French Magistrate of Justice, before the OECD Symposium on Trans-border Data Flows and the Protection of Privacy, in Vienna, Austria, Sept. 1977 quoted in Regan 1994 (52) No 3 *AJES* 260.

229 Kling and Allen "How the Marriage of Management and Computing Intensifies the Struggle for Personal

easy for organisations, companies, governments and individuals to collect, store, retrieve and manipulate personal information.[230] The exchange of personal information has become integral to the functioning of the global network economy and has made the security and privacy implications of trans-border data flows frontline issues confronting not just the developed countries, but also the developing ones.

According to the United Nations Development Programme (UNDP), today's technological transformations are intertwined with another major historic shift — economic globalisation that is rapidly unifying world markets. The two processes are mutually reinforcing. The new tools of information and communications technology reinforced and accelerated the process of trade liberalisation and privatization, which in turn accelerated economic globalisation. The economic globalisation has resulted in a global marketplace that is technology-based, with technology a major factor in market competition.[231]

5.2 Trans-border flows of trade-related information

In this global, technology-driven and interconnected economy, it is virtually impossible to confine information to national borders, because information traverses geographical boundaries without reference to a country's economic development. As information technologies increase in number, power and usage, economic globalisation encourages cross-border mergers, acquisitions, joint ventures and FDI. Companies expand their markets beyond their national borders and because of the migration of skilled labour across national boundaries, trans-border flow of data concerning employees, clients and other business-relevant information also increases. Such companies are then compelled to conform to foreign regulatory requirements concerning the use of information.[232]

Privacy" 106.

230 Regan *Legislating Privacy* 15.

231 See n 110 at 31.

232 See n 47 at 85. For example, Shaffer notes that, "[w]ere U.S. companies to operate only domestically, they would be unconcerned by the Directive. When they wish to invest, operate and trade between multiple jurisdictions, whether independently or through complex networks of affiliates and alliances, they must adapt to foreign regulatory policies."

Multinational corporations, financial institutions, airlines and credit card companies cannot function without transferring data (including personal data) between countries. Société Internationale des Télécommunications Aéronautiques (SITA), the umbrella body for the international air transport network, was the pioneer in commercial trans-border data flows. As early as 1949, eleven airlines operated a reservations system through SITA using a low-speed tele-printer system. Commercial transmissions by means of electronic networks commenced during the 1960s and 1970s, facilitating airline reservations, international banking and credit control.[233]
The trans-border flow of trade-related personal information has generated a lot of debate in recent years with particular reference to the privacy implications of such information flows. The debate often proceeds in terms of the "free flow of information" versus trade restrictions rhetoric.[234] Two main contending views dominate the debate: the European view that emphasises privacy and national control of the dissemination of personal information versus the American view that emphasises the economic imperative of free flow of information guided by self-regulation. At the heart of the two seemingly opposing views is the undeniable reality that the whole rhetoric about regulation is geared towards one purpose: the facilitation of cross-border trade.[235]

5.3 Privacy concerns raised by TBDF

Although electronic data flows across national boundaries, it is not all nations that have developed or are developing new legal strategies for regulating conduct in cyberspace or even conduct arising from the use of new technologies. Nigeria has set for itself the task of bridging the digital divide between it and the rest of the developed world as it seeks access to the global network economy. Such a task can best be accomplished by addressing the regulatory and legal issues arising from the use of these technologies. One key issue is that of information privacy and data security. The inflow of foreign direct investment into the country and the continuing

233 Hamelink *New Information and Communication Technologies* 6 [online].

234 Regan 1993 (52) *Am J Econ Sociol* 257.

235 Stewart *The Economics of Data Privacy* [online].

expansion and digitisation in the banking, oil and telecommunications industries, will see increasing inflow and outflow of personal information. It is therefore necessary to adopt a global perspective in seeking the resolution of the legal and regulatory problems inherent in the use of information technologies.

CHAPTER 3

THE NIGERIAN STATE AND SOCIETY IN THE INFORMATION AGE

> You people are all talking about downloading and uploading. We are talking about loading people's stomach and you are talking about downloading. What are you going to download? Our goal is to load food into people's stomach...[236]

1. INTRODUCTION: NIGERIA: A BRIEF HISTORY OF ITS POLITICAL AND ECONOMIC DEVELOPMENT

This chapter will examine the Nigerian state and the extent of involvement of the society in the dynamics of the Information Age. It will also examine the institutional and regulatory frameworks that will oversee Nigeria's planned integration into the global networked economy.

The Federal Republic of Nigeria lies on the West Coast of the African Continent, bordering the Gulf of Benin and having Cameroon to the east and south east, Chad to the northeast, Niger Republic to the north and Benin Republic to the west as her neighbours. It is a federal republic consisting of 36 states and a Federal Capital Territory, Abuja, in the central region of the country as the political and administrative capital. Lagos, which was the political capital until 1991, remains the economic and industrial powerhouse.

---

[236] This statement was made by the then Nigerian Presidential candidate and later President, Olusegun Obasanjo during a pre-election interview with a number of Nigerian print and electronic media journalists in 1999 who sought to know his views about Information and Communication Technologies and the Internet generally. See Famakinwa 18 Jan 2001*Thisday*.

1.1 Pre-1900-1969

British colonial influence was established in the southern and northern parts of Nigeria in 1901. From then till 1914, what is now known as Nigeria was administered by the British as two separate Protectorates.[237] By 1914, the amalgamation of the two protectorates into a single geographical and political entity, called Nigeria, arose out of the overriding need to balance the cost of administration in the northern protectorate, which was in deficit and the southern protectorate, which was in surplus.[238]

The British administrative strategy was based on the concept of indirect Rule.[239] It is generally acknowledged that this policy of indirect rule laid the foundation for Nigeria's present political instability. This policy established a pattern of separate development, which prevented a harmonious co-existence amongst the Nigerian people.[240] As Prof. Anya[241] argues, an important consequence of the divide and rule strategy was that the institutions of the state, such as the army and the economy, were designed to serve extraneous and foreign interests and were, particularly in the case of the economy, developed along different routes.[242] Nigeria became independent on 1 October 1960 and almost immediately, the weak institutional and democratic value base upon which the independent country was established, began to crack. By 1966 the whole structure crumbled when the military overthrew the civilian administration. This unleashed a series of events upon Nigeria, the effects of which culminated in a bitterly fought civil war from 1967 to 1970.

---

237 US Library of Congress *Country Studies* [online].

238 Anya *When will Nigeria take Charge of Nigeria?* [online]

239 Ibid.

240 Ibid.

241 Ibid.

242 Ibid. Prof Anya argues that the opportunities for endogenous development, growth and integration of the different nationalities and cultures were foreclosed, since they were denied the opportunities for autonomous interaction. According to him, the varied backgrounds and cultures of the new leadership that were thrown up by the fast pace of the independence struggle, created a false sense of unity grounded upon an immature institutional and value framework which could not sustain democracy.

1.2 1970-1999

It would not be far from the truth to say that Nigeria's best years were the period from 1970 to 1983. In 1970, the civil war came to an end and thereafter, an energetic programme of reconciliation and reconstruction began. Riding on the back of the oil boom of the 1970s, the economy showed very good signs of health and double-digit growth were expected to continue for a period of time. The country embarked upon gigantic and ambitious infrastructure development programmes, supported enthusiastically by the international business and financial community.[243]

The vibrant economic growth that had been witnessed in the 1970s and very early 1980s was brought to an abrupt end by the global economic crisis in the 1980s. This crisis was due in part to the rising cost of energy occasioned by high crude oil prices and consequently, in the case of Nigeria, drastically reduced incomes from the petroleum industry as a result of the oil glut. In 1986 the then military government of General Babangida sought to revamp the economy by introducing the Structural Adjustment Programme (SAP).[244] The main components of SAP consisted of exchange rate adjustments in line with market forces, deregulation of the economy, trade liberalisation, privatisation, commercialisation and diversification of the economy to harness the country's potentials in the non-oil sector. The benefits of SAP were largely illusory due mainly to the government's inconsistency and indiscipline.[245]

A new industrial policy was launched in 1998 with the aim of removing the bureaucratic bottlenecks and negative conditions that hampered foreign investment in the country. New laws[246] were promulgated and incentives announced, while the

---

243 See n 238.

244 Okome *State and Civil Society in Nigeria* [online].

245 Ibid. A peculiar feature of the SAP in Nigeria was the inconsistency in implementing the programme. For example, the reform of the foreign exchange market started in 1986 with the dismantling of exchange controls and establishment of a market-based autonomous foreign exchange market. However, a fixed official exchange rate was allowed to exist alongside the autonomous market. This anomaly exists up till today. Furthermore, the gradual market-based depreciation of the naira was stopped by the government in 1994 by means of a sharp devaluation in the official exchange rate in a bid to close the gap between the official exchange rate and the autonomous market rate. See Mkandawire and Soludo (ed) *African Voices on Structural Adjustment: A Companion to Our Continent, Our Future* 475-476.

246 In 1989, the *Nigerian Enterprises Promotion Decree* of 1977 which had tightened restrictions on foreign

government embarked on a high profile economic diplomacy through trade missions and international trade fairs. These efforts, as laudable and well thought out as they were, did not produce the much-desired result of boosting the economy. This was primarily because of the human rights abuses and corruption that have characterised Nigeria's political development under dictatorial military regimes. Under the regime of the late Sanni Abacha, the last but one military Head of State of Nigeria, the treasury was systematically looted by the man, his aides, immediate and extended family and several faceless government officials. His human rights abuses earned Nigeria the status of an international pariah state.

1.3 1999 – present day

In May 1999, Chief Olusegun Obasanjo, a retired general who was the military head of state between 1976 and 1979 when he willingly handed over power to a democratically elected civilian administration, was sworn in as president of Nigeria. This ushered in a new dispensation of civil democracy. The international community appreciated President Obasanjo and his government's efforts and determination to stamp out corruption from Nigeria's body politic. However, there were and still remain contradictions in the system.[247]

Nigeria continues to grapple with corruption, poverty, civil unrest, characterised by inter-tribal and religious clashes, fear, insecurity and massive environmental and ecological degradation, particularly in the Niger Delta. The large-scale development

---

investment in Nigeria by expanding the list of activities exclusively reserved to Nigerian investors (e.g. bus services, travel agencies, the wholesaling of home products, film distribution, newspapers, radio and television and hairdressing), was amended so as to leave a single group of 40 business activities in which foreign participation was permitted where the value of the enterprise exceeded N20 million ($2.7 million in 1989). In addition, foreign investors could only hold a share of up to 40 per cent in insurance, banking, oil production and mining. In 1995 however, the *Nigerian Investment Promotion Commission Act* opened all sectors of the economy to foreign participation except for a short negative list (including drugs and arms) and allowed for 100 per cent foreign ownership in all sectors, with the exception of the petroleum sector (where FDI is limited to joint ventures or production sharing). See UNCTAD *Investment Policy Review of Nigeria* 4.

247 The legislature, namely the National Assembly, is not seen as working in tandem with the executive arm in the drive to stamp out corruption. For example, five members of the National Assembly, including the former Senate president, as well as the former minister for education were arraigned on April 12 2005 for their alleged role in a N55 million bribe-for-budget scam. The legislators allegedly demanded N55 million bribe from the sacked minister in order to increase the budget appropriation for the education ministry. See Shehu 5th July 2010 *Thisday*.

of infrastructure embarked upon in the 1970s and early 1980s was not maintained into the 1990s; consequently, Nigeria's infrastructures remain largely decrepit.[248] The Nigerian market may be in sheer size, the largest in Africa, but in real terms it is one of the weakest.[249]

Nigeria has an estimated population of over 168 million people; it is the most populous country in Africa and the tenth most populous country in the world.[250] This will put the country among the five or six most populous nations in the world.[251] In 1983, Nigeria's GDP was US$64.57 billion and rose to US$73.45 billion between 1984 and 1985 respectively. It was ranked number 23 and 21 respectively in these two years. However, the World Bank reported Nigeria's GDP in 2012 to be US$ 262.6 billion.[252] These statistics have a direct bearing on the quality of life of Nigerians and indeed, the questions to be addressed in this work. As will be shown in the next and subsequent chapters, the high levels of population and poverty have a negative impact on the literacy level of Nigerians and therefore limit their overall capacity to access information. Without information, their capacity to make informed choices about the privacy of their information when accessed and other life choices is very limited.

From 1986/1987 on, the country was hit by the triple disaster of political instability,

---

248 The corruption and outright looting that characterized the military's years in power, resulted in a collapsed national infrastructure. The state owned monopoly responsible for generation and distribution of electricity, National Electric Power Authority (NEPA), the four petroleum refineries, Nigerian Telecommunications Limited (NITEL), the telecommunications monopoly, were all neglected over the years with the result that the supply of electricity, telephone services and refined petroleum products frequently fall short of demand.

249 Nigeria's population in 1980 was reported to be 73.6 million with a GDP of $64.2 billion while South Africa's population and GDP for the same year was 27.5 million and $80.5 billion respectively. In the year 2000, Nigeria's population reached 122.8 million and the GDP was $45.9 billion while South Africa recorded 44 million population and GDP of $132.8 billion. Nigeria's population and GDP for 2012 was 168.8 million and $262.6 billion respectively while that of South Africa for the same period was 51.1 million and $384.3 billion respectively. See World Bank *World Development Indicators* [online]. The Central Intelligence Agency (CIA) *World Fact Book* estimated South Africa's GDP per capita to be $10,700 in 2009 while Nigeria's per capita GDP for 2009 was $2300.

250 See the National Population Commission website [online]. See UNDP *Nigerian Political Economy at the Dawn of the Millennium* 10. The population is projected to grow to 440.3 million in 2025 and 913.8 million by the year 2100.

251 See United Nations Department of Economic and Social Affairs/Population Division *World Population Prospects: The 2012 Revision, Volume I: Comprehensive Tables*.

252 See World Bank *World Development Indicators* [online].

economic stagnation and the pursuit of inappropriate and ill-fated structural adjustment programmes (SAP) which obliged it to undertake repeatedly excessive devaluation of its currency. This in turn devalued its assets, productive resources and output during the decade after the introduction of the programme. One clear effect of the SAP was that in the decade when the programme was in force, there was a significant reduction in industrialisation and the attendant reduction of manufacturing.[253] The benign neglect of the past decades has resulted in making the task of managing the Nigerian economy efficiently, a difficult one.[254]

The Nigerian economy is basically agriculture-based. Since the upsurge of petroleum production arising from the oil boom in the mid-1970s, the relative share of agriculture, livestock, forestry and fishing has declined.[255] However, the sector still constitutes the main source of employment and livelihood for about three-quarters of the population notwithstanding the increased production of oil and its current dominance in the economy.[256] Nigeria remains one of the poorest oil-producing countries in the world.[257] What is more, the oil resource has become a major source of political strife in the country. The sharing of oil revenue among the three tiers of government - federal, state and local, - and among the 36 states has remained a volatile issue in the country's political agenda.[258] Although Nigeria has enjoyed

---

253 Iyoha and Oriakhi *Explaining African Economic Growth* 9-10 [online].

254 Mkandawire and Soludo (ed) *African Voices on Structural Adjustment: A Companion to Our Continent, Our Future* 475-476.

255 See n 253 at 30-35. In 1960 Nigeria was largely an agricultural country. Agriculture accounted for about 64% of output and employed over 73% of the total labour force. For the decade 1960-1969, agriculture's share of the total output of Nigeria was about 57.3% of GDP. In the period 1980-1989, the relative share of agricultural production in Nigeria's output averaged 33.4%. In the period 1990-1997, the share of agriculture fell to 29.3% of GDP (p 8).

256 See n 253 at 36. Oil production accounts for nearly 90 per cent of government revenues and 95 per cent of foreign exchange earnings. According to Iyoha and Oriakhi, although the Gowon (1966-1975), Mohammed (1975-1976) and Obasanjo (1976-1979) administrations reported impressive economic growth rates of 9.15 in 1969-71 and 12.1% in 1972, they however entrenched a culture of high dependence on one commodity, oil, in the economy.

257 See n 253 at 8. The disparity in GDP between Nigeria and other oil-producing countries such as United Arab Emirates, Venezuela, Saudi Arabia, Brazil and Indonesia clearly shows Nigeria as one of the poorest of the oil-producing states.

258 In 2005, a National Political Reform Conference called by the President to work out reform measures that would address some of the conflicts in the polity, ended on a sour note with the delegates of the oil-producing states walking out of the conference when agreement could not be reached on what they considered a fair revenue sharing formula. See Abati *Revolt of the South-South* [online].

robust economic growth in the last decade, averaging about 7.5% growth annually, unemployment, inequality and poverty remain very high and constitute serious constraints to the development of the country.[259]

One fact that stands out from the foregoing brief overview of Nigeria's political economy is that notwithstanding all the developmental deficits it contends with, Nigeria desires to actively engage with the global marketplace. To make this desire a reality, Nigeria opened her doors to foreign participation in its economic growth by repealing in 1995 the *Nigerian Enterprises Promotion Act* which had hitherto closed Nigeria's economy to foreigners. The very few areas that were open to foreign investment were closely regulated.

The *Nigerian Investment Promotion Commission Decree*, 1995 and the *Foreign Exchange (Monitoring and Miscellaneous Provisions) Decree*, 1995, are the principal laws regulating foreign investment in the Nigerian economy. Nigeria passed through a season of heavy regulation in the 60s and 70s; a period of guided structural adjustment and de-regulation in the 80s and 90s. In the first decade of the 21st century, it started the process of increasing private sector participation in economic activities so as to increase productivity, generate employment, increase and diversify its export base and improve the citizens' technological skills, thereby attracting more foreign direct investment.[260]

In a study to examine the effect of globalisation on economic growth in Nigeria between 1986 and 2003, Feridun, Olusi and Folorunsho[261] observed that given the extent of trade openness as noted above, the Nigerian economy is gaining from globalisation. According to them, the problem Nigeria faces is not that it is excluded from the global market but that it is not fully included in it.

In chapter 7 of this work, I will argue that in order for Nigeria to be fully included in the global market, one of the key tasks it must undertake will be to ensure that it

---

259 See African Development Bank Group *Nigeria Country Strategy Paper* 2-6 [online].

260 Feridun, Olusi and Folorunsho *Analysing the Impact of Globalization on Economic Development in Developing Economies: An Application of Error Correction Modelling (ECM) to Nigeria* 173-174.

261 Id at 180.

meets all the necessary global regulatory benchmarks that will enable it to operate evenly with other players in the global marketplace. It must ensure that by means of necessary legal reforms, it establishes regulatory frameworks that meet global standards in strategic sectors of the economy such as banking, financial services and telecommunications. These sectors are heavily reliant on the collection, storage, processing and transfers of personal information. More and more of these transfers are trans-border data flows between Nigeria and other countries around the world. Data protection laws enacted in countries that Nigeria trades with, such as the EU members, require Nigeria to provide adequate data protection for the personal data of their citizens and residents that may be transferred to Nigeria.

Nigeria does not have a data protection law and therefore stands the risk of being cut off from the flow of trade-related information from these countries as stipulated in their data protection laws. This potential risk calls for a careful examination of the implications for Nigeria of data protection laws and trans-border data flows in its quest for full integration into the global network economy.

1.4 Nigeria and the information society: in or out?

In the 1960s, when most of the third world countries, (particularly African states south of the Sahara), were emerging from their colonial shadows, it became axiomatic to link development with communications.[262] It was thought that this linkage between communications and development through the different means of communication would influence and change the attitudes of the "primitive" and traditional societies of Africa. This influence would in turn transform these societies into modern ones by making the people open and receptive to "modern" ideas and methods of doing things.[263]

It was on the basis of such reasoning that, for several decades, development aid agencies and institutions working in Africa and other developing countries, supported the development of information infrastructures in these countries.[264]

---

262 Mowlana *Global Information and World Communication* 188.

263 Ibid.

264 The Acacia Initiative, under the International Development Research Centre (IDRC) of Canada, is an

However, these infrastructures were unable to keep pace with the rate of advancement in the technologies that powered the dissemination of information Thus, Africa has perennially lagged behind the Western countries, separated by the "Digital Divide" that the continent is now frantically trying to bridge.

1.4.1 The digital dilemma in Nigeria

As suggested earlier in this study,[265] Nigeria needs to plug into the global networked economy. In recent years, a number of studies have been undertaken to determine the extent to which different countries interact with the "networked environment".[266] With the aid of statistical models, these studies[267] measure a country's preparedness and ability to use ICTs as tools for economic, social and technological development. The models also serve as benchmarks for measuring a surveyed country's progress over a period of time as well as a basis for comparative assessment of each country's readiness to use technology for development. The comparisons yield a composite index of rankings assigned to each of the surveyed countries. According to the Economist Intelligence Unit:[268]

> E-readiness is not simply a matter of the number of computer servers,

---

international program to empower sub-Saharan countries with the ability to apply ICTs to their social and economic development. See IDRC *Acacia Initiative* [online]. The International Institute for Communication and Development (IICD) also assists developing countries to utilise the opportunities offered by ICTs for sustainable development. See the IICD website [online]. The Leland Initiative under the auspices of the United States Agency for International Development (USAID) is involved in bringing the benefits of the global information revolution to the people of Africa, through connection to the Internet and other Global Information Infrastructure (GII) technologies. See USAID Website [online].

265 See chp 1 par 1.5.

266 See Information Technologies Group *Readiness for the Networked World: A Guide for Developing* Countries 7.

267 The Networked Readiness Index (NRI) was first published in 2002 and reviewed the years 2001-2002. It was published again in 2003 covering the years 2002-2003. The 2005 index, covers the years 2004-2005. Another survey, the *Global E-government Readiness Report 2005: From E-government to E-inclusion* (2005), is a study commissioned by the United Nations organisation to assess different countries according to their state of e-government readiness and the extent of e-participation worldwide based on website assessment, telecommunication infrastructure and human resource endowment. Previous reports were published in 2003 and 2004 and all reports are available at the same website. See also Economist magazine *The 2005 E-Readiness Rankings* [online]. *The 2005 E-Readiness Rankings* is a survey by the Intelligence Unit of the *Economist* magazine. There are also reports for 2002, 2003 and 2004.

268 See n 267.

> websites and mobile phones in the country (although these naturally form a core component of the rankings), but also such things as its citizens' ability to utilise technology skilfully, the transparency of its business and legal systems, and the extent to which governments encourage the use of digital technologies.[269]

Nigeria's rankings in these surveys clearly indicate a poor network environment.[270] This is understandable given the low level of human development[271] and the marginalising effects of poverty and political instability. Poverty in Nigeria is broad, deep and on the increase.[272] Africa as a whole has in the last 45 years been haunted by the dilemma of choosing appropriate, viable and sustainable development programmes that would best meet the needs of its severely disadvantaged nationalities.[273]

For Nigeria, this dilemma is perhaps best exemplified by the comments of Peter Enahoro, the veteran Nigerian journalist, when he said:

> We now have some of the best roads in the world, but it is questionable

---

269 Ibid.

270 The Networked Readiness Index Rankings for the years 2001-2005 show Nigeria declining from the 75th position in the 2001-2002 survey to 86th position in the 2004-2005 survey. The Economist Intelligence Unit's e-readiness rankings for Nigeria in the years 2002-2005 are 55, 55, 58 and 58 respectively, indicating a marginal decline.

271 The *Human Development Index* for 2002 shows Nigeria occupying the 155th position out of 177 nations ranked. See the United Nations Development Programme (UNDP) *Human Development Report 2004*. The Report also shows that *The Human Poverty Index* (HPI-1) value for Nigeria is 35.1%, ranking her 57th among 95 developing countries for which the index has been calculated. The human development index (HDI) focuses on three measurable dimensions of human development: living a long and healthy life, being educated and having a decent standard of living. It combines measures of life expectancy, school enrolment, literacy and income to allow a broader view of a country's development than does income alone.

272 In February 2012, the National Bureau of Statistics, the main statistical agency and custodian of official statistics in Nigeria, declared that 112.519 million Nigerians live in relative poverty conditions. See Onuba February 14th 2012 *Punch.*

273 This dilemma was in part caused by the antecedent history of most of the African states that had been under colonial domination for centuries and whose histories were distorted by their colonial administrators. The political structures necessary for the effective delivery of sustainable development are still in the process of being laid out. It is for this reason that McAnany concluded that "the approach to a 'solution' to the problems of the rural poor is a political one, rooted in the history of the country and the structures that continue to support the status quo". See McAnany E G (ed) *Communications in the Rural Third World: The Role of Information in Development* 11; see also Stover W J *Information Technology in the Third World: Can IT Lead to Humane National Development?* 21.

> whether the money we spent building new expressways should have been used that way... Nigeria imports millions of dollars' worth of rice, yet we are a tropical country and could grow our own food. On the other hand, if we had not built highways, someone would say, they have magnificent mechanised farms but they cannot transport their produce... So there is a debate over whether we have chosen the proper priorities.[274]

The choice of proper priorities continues to plague the Nigerian state; like many other African countries south of the Sahara, the country is still struggling to provide the basic necessities of life such as food, shelter, safe drinking water and basic health care services. In addition, the provision of infrastructures such as schools, roads, electricity, hospitals and housing continue to cry for urgent attention in the face of the long ignored decay of such facilities or their non-existence. Apart from these challenges, Nigeria is also confronted with the Information Revolution and must therefore determine the right priorities in sharing the limited resources available between the provision of the basic needs of life and the demands of the Information Revolution.

This is all the more challenging given that the convergence of computers and telecommunications, together with all the other new information and communications technologies are now touted as the springboard for Africa's development:

> These technological developments in networking and communication infrastructure are not a luxury - they are a priority for Africa as they comprise considerable and tangible stakes: stakes of power, because nowadays being on the information highway gives power; economic stakes because of the huge investments involved with new information technologies; technological stakes in the choices being made over infrastructures and methods of connection in Africa; and stakes in research sector to develop the new information technologies according to the priorities, needs and expectations of the African Continent.[275]

The Information Revolution has in the last thirty years experienced a growth factor never seen before, powered chiefly by advances in technology which have given rise

---

[274] Quoted in Stover *Information Technology in the Third World: Can IT Lead to Humane National Development?* 21.

[275] De Roy 1997 (18) Issue 5 *TWQ* 892.

to smaller and more powerful processor chips that drive the ICTs today.[276] Developing countries are increasingly adopting these new technologies with the result that many of them have witnessed a paradigm shift in the focus of their development goals. The basis of wealth creation and prosperity is turning from natural resource dependency to the knowledge-based and technology driven model in which skills and knowledge, sharpened and facilitated by information and communication technologies, are now the basis of comparative and competitive advantage at the national and global levels. Countries like Singapore, South Korea, Malaysia, India and Brazil, are some of the countries that have witnessed a transformation of their economies as a result of embracing ICTs as tools for development.[277]

Nigeria comes into this revolution with obvious infrastructural, human resources and regulatory deficits; and yet, to ignore the evident advantages of these technologies and the opportunities they provide and empower for meaningful national development would be a grievous mistake. It is for this reason that the country adopted a forward looking *Information Technology Policy* that sets out:

> To make Nigeria an IT capable country in Africa and a key player in the Information Society by the year 2005, using IT as the engine for sustainable development and global competitiveness[278]

Although the year 2005 has come and gone and it cannot be said that Nigeria has become the IT capable country envisaged in the policy document, the vision expressed therein continues to be relevant to the country's development goals. In fact, in one area of IT usage, namely mobile telecommunications, Nigeria has recorded tremendous growth which has impacted virtually every area of the country's economy.[279]

---

276 Maherzi *World Communication Report: The Media and the Challenge of the New Technologies* 30.

277 According to Manyika and Roxburgh, the Internet contributed 7% of growth in emerging economies such as Brazil, India and China over the past 15 years and 11% over the past five. In countries such as Turkey, Malaysia and Mexico, where both Internet usage and GDP per capita fall within the medium range on the global scale, the Internet has also contributed substantially to economic growth, though to a lesser degree than in mature economies. See Manyika and Roxburgh *The Great Transformer* 3 [online].

278 NITDA *National Policy for Information Technology* iii [online].

279 As at August 2011, the total number of connected fixed and mobile lines in Nigeria was 120,331,481 while

While Nigeria continues to grapple with the major challenges of poverty alleviation, an evolving democracy and balancing ethnic tensions, the nation must make every effort to participate in the Information Revolution. Nigerian policy-makers have come to realise that the nation cannot continue to rely solely on its natural resource base for much longer. The country has therefore set its eyes on bridging the digital divide that is so evident in the various e-readiness reports highlighted earlier.

According to the Economist Intelligence Unit, publishers of the *Digital Economy Rankings and Scores, 2010* (formerly known as e-readiness rankings):

> Given the prevalence of Internet-connected consumers, businesses and governments, and the indispensable role that digital communications and services now play in most of the world's economies, we believe that the countries in our study have achieved, to one degree or another, a state of e-readiness. The study's new title, the "digital economy rankings", captures the challenge of maximising the use of information and communications technology (ICT) that countries face in the years ahead. (Underlining supplied).[280]

The telecommunications industry is the powerhouse of any digital economy. Nigeria's remarkable improvements in the telecommunications sector of the economy attest to the EIU's belief that Nigeria, like the other countries surveyed, has attained a measure of digital readiness. Nigeria's e-readiness or digital economy rankings of 61 in 2009 and 2010 respectively are lower than Malaysia's, another developing country, with a ranking of 38 and 36 for 2009 and 2010 respectively. Nevertheless, they demonstrate a measure of digital economy readiness that should persuade Nigeria's policy makers to vigorously address the challenges of maximising the use of ICTs as noted in the EIU 2010 Report. One of such challenges is developing a regulatory environment for the use of ICTs in Nigeria that will be able to interface seamlessly with the regulatory requirements of the global networked economy.

---

the total installed capacity of fixed and mobile lines were 164,918,991. See NCC *Monthly Subscriber Data* [online].

280 Economist Intelligence Unit *Digital Economy Rankings 2010* [online].

2. KEY ISSUES IN NIGERIA'S COMPUTER AND INTERNET PENETRATION

2.1 Introduction

Bringing Nigeria into the global network economy will not be easy, but it is also not impossible. It is undeniable that national capability in science and technology is vital for the socio-economic progress of developing countries such as Nigeria, whose economies have for long been dependent on natural resources. With the current shift in global economic focus from resource-based to knowledge-driven economic activities, the great potential of science and technology, particularly information technology, for sustainable economic development is now commonly accepted.

Information technology, of which the Internet and the enabling ICTs are the key components, requires capital-intensive investments. This fact prompted the likes of Jason Pontin of *Redherring* magazine to discount information technology (IT) as irrelevant, not only because of the other basic and more pressing needs like food and water, but also because, as he puts it, "... they [the poor nations] would not know what to do with it".[281]

This view calls into question whether poor regions of the world like Africa can in general benefit from the diverse uses of the Internet and whether there is anything that they can contribute. As the former Nigerian President asked, is Africa only "downloading" or does it have a chance to "upload" as well?[282]

Pontin, in an editorial column titled "The Wretched of the Earth", opined that ICTs

---

[281] The article was published in the *Red Herring* online magazine in 2000 [online]. It was first accessed by this writer on 12/4/01. Although the magazine is still published online, the particular article is no longer available. However, see Pontin *New economy does not mean laws of economics have overturned* [online] in which he referred to his article "The Wretched of the Earth" and his comment about Ethiopia.
See also Molla *Africa and the Information Economy*1 [online].

[282] See n 236. The question is very relevant, depending on how one looks at it; in the context of development aid, will Africa reach the point where it will be the source of development aid (uploading) to other regions of the world, or will it continue as a perpetual recipient of aid (downloading)? In the context of the Internet/e-commerce, will Africa perpetually rely on software import/input and information, education and entertainment content from external sources (downloading), or will it also be able to contribute, if not the hardware, at least the software and rich content for the Internet/e-commerce (uploading)?

would not make any difference to developing countries like Ethiopia.[283] He argued that two things are wrong with the "triumphalist millenarianism" thinking that poor countries can leap-frog certain stages of development with a view to "take their place in a global economy". For one thing, he argues, "it is at odds with the reality of life in a very poor country" and secondly, "it is at odds with economic theory". He concludes that countries need education, health, water, food, roads, foreign investment, political liberties, etcetera and not information technology.[284] His rationale for such comments is his belief that information technology can do nothing for poor countries because these countries "wouldn't know what to do with technology even if they could afford it".[285]

Notwithstanding Pontin's dismissive conclusion, Molla argues that some form of local information economy capacity is vital for economic development in the poor countries of the world. This is because economic activities across the world will continue to be powered by ICTs both now and in the future. In addition, he adds, it is a commonly accepted notion that if a country can afford it, there can be no better alternatives or options to ensure development, than relying on indigenous capacities.[286] For Nigeria, as indeed for the whole of Africa and other developing countries, the sobering reality is that they run the risk of becoming part of what Castells calls "the Fourth World" which "is composed of people, and territories, that have lost value for the dominant interests in informational capitalism".[287]

I believe that ICTs and the Internet are very crucial for Nigeria's socio-economic development and clearly indispensable in its bid to become fully integrated into the global economy. Pontin's contention that poor countries need education, health, water, food, roads, foreign investment, political liberties, etcetera and not information technology is a very simplistic view of what poor countries need. Take

---

283 Jason Pontin, the then editor of *Red Herring* magazine, wrote his article after a visit to an Ethiopian village in March 2000.

284 Ibid.

285 Ibid.

286 Molla *Africa and the Information Economy* 7 [online].

287 Castells *Information Technology, Globalization and Social Development* 18 [online].

education for example; any poor country that aspires to educate its population without recourse to advances in science and technology is wasting its meagre resources because in the end, that country's population will be educated but not knowledgeable. If a university in such a country offers a degree programme in computer science and the students have no access to computers or perhaps they are acquainted with only the first generation personal computers with obsolete technology, one wonders what value such students would add to the domestic and international economies.

The application of ICTs to the fundamental needs of the society makes the provision of the basic needs more efficient, cost-effective, productive and more widespread, including political liberties.[288] Obviously ICTs cannot solve all the problems of humanity but they do provide tools that enable us to more efficiently and quickly tackle the problems we are able to deal with. Even Pontin will agree that these technologies are already deployed for various uses in poor countries. Indeed, there is no way a poor country can, in the 21st century, construct roads, build health-care facilities and schools and provide other so-called basic necessities of life without recourse to ICTs either to plan, implement or maintain the provision of such necessities. In the case of Nigeria, the question is no longer "if" it needs ICTs but how quickly can they be deployed.

Information and communications technologies encompass the full range of the production, distribution and consumption of information, across all media from radio and television to satellites and the Internet.[289] Nigeria recognises information technology as a fundamental pre-requisite for national survival and development within the context of a rapidly changing and networked world.[290] As a developing country which must participate effectively and ensure a key position in the emerging Information Age, Nigeria requires an effective and efficient IT system organised around an appropriate IT policy.

---

288 The Egyptian Revolution in January 2011 for example, achieved a critical mass because of the use of ICTs such as mobile phones, the Internet and the social network sites like Facebook and Twitter. These tools enabled the population to gain political freedom.

289 Wilson *Globalization, Information Technology, and Conflict* 6 [online].

290 See the *National Policy for Information Technology* ii-iii [online].

The Federal Government of Nigeria approved the National Information Technology Policy[291] in March 2001, and in April 2001 set up the National Information Technology Development Agency (NITDA) to implement the Policy.[292] The vision of the policy is to make Nigeria an IT - capable country and a key player in the Information Society, using IT as the engine of sustainable development and global competitiveness. A target date of 2005 was set for realising the vision.[293] The government accepted IT as a strategic imperative for national development because of its immense benefits. The policy was anchored on the advancement of information technology through research and development activities, in order to create and support a knowledge-based society that can exploit information resources.

The latter part of the twentieth century was characterised by the phenomenal explosion in IT and all of its enabling technologies, but the world does not wait for any group to catch up. It is doubtful that Nigeria can attain the same level of technological advancement today that a country like the United States of America took the whole of the last century to achieve. However, and herein lies the advantage for Nigeria and indeed other less developed countries, there is no need to invent the wheel again. What took other countries hundreds of years to achieve need not take as long for these less developed countries for there is now a window of opportunity for these nations to enter into the Digital Age in the shortest possible time. This opportunity can best be utilised by enabling a knowledge-based and knowledge-driven economy through the careful provision of a legal and infrastructural framework that will support the transition from perennial poverty alleviation to wealth creation.

---

291 Ibid.

292 Ibid.

293 As said, the objective of the policy to make Nigeria a key player in the Information Society by the year 2005 has not yet been realised. Notwithstanding Nigeria's performance in the e-readiness rankings referred to in fn 281 above, some progress has been made in terms of technology acquisitions particularly in the telecommunications sector, since the adoption of the policy in 2001. Nevertheless, there is still a long way to go in bridging the digital divide and effectively regulating the flow of information into and out of Nigeria.

2.2 Development of information technology in Nigeria

The United Nations Development Programme (UNDP) has noted that the number of computers in a country is one of the indicators for measuring productivity, competitiveness and human development.[294] The lower the number of computers, the lower the level of output and the lower the level of national income available for improving the political, social and economic well-being of the people.[295] The history of IT in Nigeria can be traced to the 1962/1963 population census when the first electronic computer used in Nigeria was purchased for the purpose of analysing the census data.[296] Since then, information technology development in Nigeria has passed through four distinct phases, namely: the early phase from 1963 to about 1975; a period of computer consciousness from 1977 to 1982; followed by a period of relative stagnation from 1982 to 1993 and lastly, a period of new upsurge in the acquisition and use of computers from 1994 to the present day.[297] Indeed, it can be said that the period from 1999 to the present has witnessed the greatest uptake of ICTs in Nigeria's history.[298]

2.3 Computer usage

It is estimated that between 1963 and 1973, the total number of computers in the country was less than twenty five, with about six of these being associated with the multinational companies. By 1977 there were estimated to be about 115 computers altogether.[299] The second phase of computer penetration in Nigeria (between 1977 and 1988) witnessed an increase in computer usage particularly by institutions such as universities, government departments and government-owned or funded

---

294 UNDP *Human Development Report* 2001 52.

295 Ibid.

296 Nwachukwu *Development of Information Technology in Nigeria* [online].

297 Ibid.

298 For example, in 1999 there was only 1 national carrier, 9 Private Telecommunications Operators (PTOs) providing fixed telephony, 25 VSAT networks and 18 ISPs, whereas in 2004, there were 2 national carriers, 24 PTOs providing fixed telephony, 52 VSAT networks and 36 ISPs in Nigeria. See Ndukwe *Country Experience in Telecom Market Reforms- Nigeria* [online].

299 See n 296.

organisations like the West African Examinations Council (WAEC), the Joint Admissions and Matriculation Board (JAMB), the National Electric Power Authority (NEPA), the Nigerian Ports Authority (NPA) and the Federal Office of Statistics. Banks and commercial firms also began to show interest in computers during this period. The total number of computer installations in Nigeria in 1988 was 754 out of which 177 were industrial installations.[300]

In 1988 the Nigerian government introduced computer literacy studies into the secondary school curriculum as part of the efforts to develop the skills required for a computer-literate society. The National Universities Commission (NUC) and the National Board for Technical Education (NBTE) articulated and complemented the efforts of the government by introducing courses in computer literacy in the institutions under their control.[301] Minimum standards set by the National Universities Commission currently require every university student to take computer science courses at the 100 level.[302] As a result, there has been a marked improvement in the number of computers and trained personnel in Nigeria, although such improvement still falls far short of global benchmarks.[303]

2.4 Internet penetration

The Internet has already made considerable inroads into the Nigerian socio-economic landscape. At present, there is no real e-commerce culture and platform in Nigeria. This is not because of a lack of interest in e-commerce, but because of the fact that a critical mass in networking and telecommunications infrastructure has not yet been attained. Nigeria remains one of the lowest rated African countries in terms of Internet and computer usage.[304]

---

300 See n 296.

301 Alabi *Empowering Socio-Economic Development in Africa* 29 [online].

302 Ibid.

303 See chp 1 par 1.5 above. According to the National Bureau of Statistics, 4.5% of the national population has access to computers while only 0.9% of the population actually own a computer. See *Businessday* 1st January 2013.

304 See Harvard University Center *Global Information Technology Report* 11 [online]. At the end of 2004, there were an estimated 1.6 million Internet users in Nigeria, according to the NCC. See also Ndukwe *Country Experience in Telecom Market Reforms – Nigeria* 17 [online]. In 2010 however, the ITU

Access to the Internet in Nigeria is growing, because of the continuing fall in the cost of bandwidth and equipment, particularly in the telecommunications sector. Undoubtedly, without telecommunication technologies (such as the telephone and modem) the Internet would not be possible. The rapid increase in telephone density in Nigeria has powered the growth of Internet usage. As a result, more large and medium sized businesses in the urban centres are increasingly using the Internet. However, one of the biggest constraints to the growth of Internet usage is the limited availability of data-capable telephone lines; the result is that large numbers of cyber-cafes are being opened in the urban centres of Nigeria. In 2005, there were 38 Internet Service Providers licensed by the Nigerian Communications Commission (NCC), the telecommunications regulator, to sell Internet services, but by March 2012 the number had increased to 123 ISPs.[305]

Notwithstanding the above mentioned constraints, some exciting developments that have taken place in the corporate sector are signalling the dawn of the Internet age in Nigeria. For example, a good number of the leading newspapers and magazines have registered their presence on the Web.[306] However, the most far-reaching developments have taken place in the banking and telecommunications sectors, with Internet banking now firmly established and expanding in scope. In the past five years, banks in Nigeria have increasingly turned their attention to deploying IT tools to enhance their services and therefore productivity.[307]

Virtually all banks in Nigeria now offer on-line, real-time banking services. The few unable to do so are losing their customers. The massive introduction of technology into the banking industry has given rise to new and imaginative banking services and products. For example, customers now have the flexibility of operating their accounts at any branch of a bank irrespective of where the account was opened. The advent of

---

estimated that about 43million Nigerians use the Internet. See Ahiuma-Young 5th August 2010 *Vanguard* newspaper. See also ITU ICT *Statistics* [online].

305 NCC Report *Trends in Telecommunications Markets* [online]. As of 1st March 2012, there were 123 ISP registered by the NCC. See NCC website [online].

306 The Guardian [online], the Vanguard [online], the Punch [online], Thisday [online], Newswatch magazine [online] amongst others.

307 Ovia "Internet Banking: Practices and Potentials in Nigeria" [online].

the Internet and global e-commerce and their adoption by the Nigerian banking industry, has led to radical changes in Nigeria's financial landscape with most of these banks now represented on the Internet.

2.5 Electronic/Internet banking

Electronic banking involves the use of automated processes and electronic devices[308] in banking transactions. Some banks practice electronic banking for informational purpose, some for simple transactions such as checking account balance as well as transmission of information, while others facilitate funds transfer and other financial transactions. Many systems involve a combination of these capabilities.[309] A survey conducted in September 2002[310] to determine the level and types of e-banking activities carried out by banks in Nigeria, showed that seventeen banks were offering Internet banking, twenty four were offering basic telephone banking, seven had ATM services, while thirteen of the banks indicated that they were offering other forms of e-banking. Twelve of the banks indicated that their websites were hosted in Nigeria, while twenty two were hosted overseas. Fourteen of the websites provide information only; eleven were information transfer systems, while twenty two were transactional in nature. Twenty seven of the banks indicated that they had security policies relating to e-banking, while four reported that they had none in place. Thirty of the banks reported that they used authentication as a means of security control, twenty eight used firewalls, sixteen cryptography, eight use digital signatures, fourteen digital certificates, eighteen used Secured Socket Layer (SSL), fifteen, Public Key Infrastructure (PKI), and thirty one mainly used physical security.

2.6 Financial services

Another remarkable development in Nigeria in relation to the Internet is the introduction of "plastic" or electronic money. A consortium of thirty one Nigerian banks recently set up Smartcard Plc, to promote a non-cash culture among

---

308 Eg, personal computers, telephones, fax machines, Internet, card payments and other electronic channels.

309 Central Bank of Nigeria *Report of the Technical Committee on Electronic Banking* [online].

310 Ibid.

Nigerians. This is a critical element in the e-commerce environment. The pilot scheme, which was launched in June 1999, was targeted at organised markets, merchants and the urban middle-class account holders in the participating banks. It was estimated that by the year 2000, the participating banks would have invested close to 1 billion Naira (Nigerian currency), to get the plastic money project going.[311] Valucard, as the plastic money is called, has been so well received that its acceptance engendered competition in the form of SMARTpay, promoted by Gemcard Ltd, a company which is also heavily backed by the banking industry.

ICTs have had a great impact on service delivery in the financial sector of the Nigerian economy. These developments have, however, not been matched with appropriate legislation or regulation to address the resultant changes in the relationships, responsibilities, liabilities and rights of the parties engaged in electronic banking. These rapid modernisation programmes have also given rise to security and regulatory concerns which need to be addressed. The banking industry and its regulatory authorities, the Central Bank of Nigeria and the Nigerian Deposit Insurance Corporation of Nigeria, need to carefully monitor the security implications of the rapid explosion in online banking.[312]

---

311 Ademiluyi 11th December 2000 *TELL* (magazine) 52-53.

312 The Central Bank of Nigeria released its *Guidelines on Electronic Banking in Nigeria* [online] in August 2003. Detailed and specific guidelines were given by the apex Bank for the security of online banking transactions. Interestingly however, under item 1.5 Standards on Security and Privacy, no single guideline was given on privacy. There seems to be a confusion of security with privacy; it should not be so because they are two distinct issues. While security issues are usually dealt with by cybercrime laws, privacy issues are dealt with by data protection laws. This lacuna concerning information privacy at the level of the Central Bank/banking industry is also evident at the national level; even though the government acknowledges the need for data protection in the IT Policy document for example, no data protection has been enacted so far to give effect to the recognised need. Even the news media appear to be more focused on the need for network security than information privacy. See Aragba-Akpore 23rd November 1999 *The Guardian* 41. According to Aragba-Akpore:

> Corporate intranets and Internet-based delivery of banking services will inevitably play an increasingly important role in the banking industry over the next several years… Intranets are already becoming a primary vehicle for internal sharing of information and resources, and the Internet is likely to be the primary delivery channel for PC-based electronic banking services to both retail and corporate customers… Consequently, the banking industry will need network security solutions that make the Internet as secure as their private networks. Strong security will guarantee the privacy of customers' information as it sails through cyberspace, as well as secure servers and network devices from unauthorized access.

3. ACCESS TO THE INFORMATION SOCIETY IN NIGERIA

3.1 Telecommunications infrastructures

No modern economy can be sustained without an integrated telecommunications and information technology infrastructure. Access to telecommunications is therefore critical to the development of all aspects of a nation's economy, including manufacturing, banking, education, agriculture and government.

It follows that a modern, viable and well-managed telecommunications sub-sector is a necessity for integration into the global network economy. The biggest problem facing Nigeria in this area is the very high cost of providing cutting-edge technology, which the weak economy cannot finance. Recourse has therefore been had to the international business community for foreign investment. To facilitate this, there must be sufficient deregulation of the industry to allow for foreign participation. Deregulation of the telecommunications sector is the avowed policy of the government.[313]

3.2 Overview of telecommunications development

Under colonial rule, the British colonial administration was responsible for the provision of telecommunications facilities; a department of Posts and Telecommunications (P&T) was mandated to provide facilities for posts and telegraph and telephone services. In 1851, a post office was established in Lagos and by 1856, the Cable and Wireless Company of the UK had commissioned a submarine cable link between Lagos and London.[314] The amalgamation of the Northern and Southern protectorates of Nigeria in 1914, resulted in the merger of the posts and telecommunication networks to form the basic national network.[315]

With independence in 1960, the P&T became a department under the Ministry of Communications and assumed responsibility for network operation and service

313 See Ministry of Communications *National Policy on Telecommunications* (2000).

314 Ige Evolution *of the Telecommunications Industry* 17 [online].

315 Ibid.

provision.[316] In 1961, the Wireless Telegraphy Act[317] was enacted to regulate telecommunications operations in Nigeria. Upon attaining independence in 1960, Nigeria had less than 20,000 telephone lines in use. In the period 1960-1985, the telecommunications sector was made up of the Department of Posts and Telecommunication (P&T) responsible for internal telecommunications, and the Nigerian External Telecommunication (NET) Limited, responsible for external telecommunications services.[318]

The telecommunications sector was commercialised in 1985 and as a result the postal and telecommunications functions of the P & T department became separated. Postal functions were assigned to the Nigerian Postal Service (NIPOST), while telecommunications functions came under the purview of the Nigerian Telecommunications Company Limited (NITEL), a fully owned government monopoly operator. NITEL is an amalgamation of the telecommunications arm of the old P&T and the then Nigerian External Telecommunications (NET).

By the year 1987, the installed capacity of telephones in Nigeria was 400,000 lines while connected lines stood at between 205 000 and 250 000 lines.[319] What this indicates is that the subscriber base grew at an average rate of about 10 000 lines per annum nation-wide over the period of twenty seven years. In 1992, cellular service[320] was commenced in Nigeria and the number of cellular lines actually connected as at December 2000 was approximately 35 000, representing an average annual growth rate of only 1 250 subscribers per annum, a most regrettable situation.[321] In April

316 Ndukwe *Evolution of the Telecommunication Industry in Nigeria* [online].

317 Laws of the Federation of Nigeria 1990.

318 See n 316.

319 Ibid.

320 Ndukwe *Country Experience in Telecom Market Reforms- Nigeria* 26 [online].

321 Ibid. According to Ndukwe, two main reasons account for the slow development of the telecommunications sector in the past:

- Government ownership of a monopoly telecommunications company, which did not give room for competition and expansion.
- Inadequate funding of telecom infrastructure development. The lack of private sector participation resulted in poor funding of the required infrastructure development as government alone could not allocate all the needed resources in the face of competing demands from other sectors of the economy.

2000, the Board of the Nigerian Communication Commission (NCC) was inaugurated following the establishment of the Commission to regulate the telecommunications industry in Nigeria.[322] The period between April 2000 and April 2005 has been described as the era of Telecommunications Revolution in Nigeria.[323]

This period witnessed a massive growth in subscriber lines from less than 25 000 analogue mobile lines in May 2000, to about 12.8 million digital mobile lines by end of May 2005. Fixed lines also grew from about 450 000 lines to over 1.2 million lines during the same period, giving a total subscriber level of about fourteen million lines.[324] An even greater surge of subscriber lines took place between the period of 2005 and 2010. According to the NCC, the installed capacity in the industry as at December, 2010 stood at 157 839 million lines, while tele-density increased to 63.11% in the same period.[325] From the foregoing, it is obvious that Nigeria has made remarkable progress in telecommunications development.

However, if the impressive figures above are compared with the country's current population figure of about 167 million people[326], it is evident that Nigeria is in need of more telecommunications facilities.[327] It is estimated that about 73 million Nigerians, representing about 46.7 per cent of the population, are yet to be provided with access to telephone services by the operators. This group is made up of those residing in the core rural and semi-rural areas of the country.[328]

---

322 The Commission was created under the Nigerian Communications Act, 1992. This Act was repealed by the Nigerian Communications Act, 2003.

323 Ndukwe *Telecommunications in Nigeria: The Next Frontier* [online].

324 Ibid.

325 The Nigerian Communications Commission *Monthly Subscriber Data (September 2010 – August 2011).*

326 Nigeria's population officially reached the 167 million mark on 31st October 2011. See the National Population Commission of Nigeria website [online].

327 According to the NCC, there were 5 GSM network operators, 4 CDMA network operators and 16 fixed/fixed wireless operators in the Nigerian telecommunications industry as at June 2011. See NCC *Quarterly Summary of Operator Data* 1 [online].

328 Nurudeen 6th January 2012 *Daily Trust* newspaper.

4. REGULATORY INFRASTRUCTURE FOR TELECOMMUNICATIONS AND INTERNET USAGE

4.1 Introduction

The telecommunications industry in Nigeria first came under official regulation in 1916 with the enactment of the *Telegraphs Ordinance* of the same year to regulate the construction and working of telegraph lines for the purpose of telegraph communication. The industry has so far been regulated through the following statutes:

- The Wireless Telegraphy Act[329],
- The Posts and Telecommunications Proceedings Act[330],
- The Telecommunications and Postal Offences Decree[331] and,
- The *Nigerian Communications Commission Decree*.[332]

The above laws primarily create offences relating to the use of telecommunications services and facilities, and outline procedures for the punishment of those offences. While some of the laws were made under military regimes[333] and reflect the military's influence, efforts have been made to reform the industry and bring the regulatory regime in line with the new democratic dispensation.

A new Act,[334] was enacted by the civilian democratic government of Olusegun Obasanjo to reform the Nigerian Communications Commission and repeal the earlier statutes that regulated the industry.[335] Consequently, two main statutes now regulate

---

329 Laws of the Federation of Nigeria, 1961.

330 Laws of the Federation of Nigeria, 1990.

331 Laws of the Federation of Nigeria, 1995.

332 Laws of the Federation of Nigeria, 1992.

333 The Telecommunications and Postal Offences Decree No 21, Laws of the Federation of Nigeria, 1995; the Telecommunications and Postal Offences Decree *(Amendment) Decree* No 19, Laws of the Federation of Nigeria, 1997; the *Nigerian Communications Commission Decree* No 75, Laws of the Federation of Nigeria, 1992; and the Nigerian Communications Commission (Amendment) Act, Laws of the Federation of Nigeria, Laws of the Federation of Nigeria, 1998.

334 The Nigerian Communications Commission Act, Laws of the Federation of Nigeria, 2003.

335 Ibid.

the telecommunications industry today.[336]

4.2 Institutional framework

4.2.1 Introduction

Prior to the establishment of NITEL in 1985, the Ministry of Communications was responsible for the planning, project execution, operation and maintenance of telecommunication facilities, as well as provision of services. The regulation of the industry under the enabling statutes was the responsibility of the Ministry. Upon the creation of the Nigerian Communications Commission (NCC) in 1992,[337] the policy formulating responsibility of the ministry was separated from both the operating and regulatory activities in the industry and vested in the NCC. The telecommunications industry in Nigeria now consists of the following operatives:[338]

- The Ministry of Communications Technology
- The Nigerian Communications Commission
- Nigerian Telecommunication Limited (NITEL)
- The Second National Operator – Globacom
- Other licensed private telecommunication operators and service providers
- National Frequency Management Council (NFMC)

4.2.2 The Ministry of Communications Technology

The regulatory regime in the telecommunications industry in Nigeria was directly supervised by the government of Nigeria through the old Ministry of Communications. The functions of the Ministry of Communications are now vested in the new Ministry, the Ministry of Communications Technology. The new Ministry also supervises the various agencies mentioned above. The role of the Ministry in the telecommunications sector includes:

---

336 The *Wireless and Telegraphy Act*, 1961 and the Nigerian Communications Act 2003. See the Nigerian Communications Commission website [online].

337 See n 320.

338 Ndukwe *Nigerian Telecommunications Environment* [online].

- Giving overall directions for telecommunications development;
- Ensuring policy consistency of telecommunications with other national policies;
- Enacting the necessary laws and taking other measures promptly in support of the national telecommunications policy.[339]

The Ministry of Communications Technology is responsible for formulating broad telecommunications policy objectives. Its activities include, amongst other things:

- Proposing policy options and recommending appropriate legislation to government;
- Implementation of government policy;
- Representing the government on matters pertaining to regional and international organisations such as the International Telecommunications Union (ITU), Pan African Telecommunications Union (PATU), International Maritime Satellite (INMARSAT) and International Telecommunications Satellite (INTELSAT);
- Overall monitoring of the radio spectrum allocation in the country.[340]

At independence in 1960, the P&T was the department under the Ministry of Communications providing and regulating telecommunications services in Nigeria. When the Wireless Telegraphy Act was enacted in 1961, it vested wide powers of control over telecommunications services in the Minister of Communications. The Wireless Telegraphy Act and the *Wireless Telegraphy Regulations* made pursuant thereto were the principal legislation regulating the telecommunications industry up to 1998 when the Act was amended.[341] The amendment transferred the powers exercised under the Act by the Minister of Communications to the Nigerian Communications Commission, to the extent that such powers related to telecommunications. The powers under the Act relating to broadcasting were also transferred to the Nigerian Broadcasting Commission (NBC). The regulatory oversight functions of the Ministry of Communications are now vested in the NCC.

---

339 Ibid.

340 See n 313.

341 Wireless *Telegraphy (Amendment) Act*, Laws of the Federation of Nigeria, 1998.

The role of the old Ministry of Communications was reduced to policy-making with the enactment of the Nigerian Communications Act in 2003.[342] In 2006, the Nigerian government under President Olusegun Obasanjo, merged the Ministries of Information and National Orientation and the Ministry of Communications into what is today the Ministry of Information and Communications. The policy-making role of the then Ministry of Communications were transferred to the Minister of Information and Communications.

Although the Nigerian Communications Act, 2003 effectively established the NCC as the primary regulatory authority over the telecommunications industry, the NCC nevertheless remained under the supervision of the Minister of Information and Communications, functioning more or less as one of the departments under the Ministry. The Act requires the Minister to indicate the general direction of government policy to the Commission while ensuring the protection of its independence. Section 25 of the Act provides:

> (1) Subject to subsection (2) of this section, the Minister shall, in writing, from time to time notify the Commission of and express his views on the general policy direction of the Federal Government in respect of the communications sector.
>
> (2) In the execution of his functions and relationship with the Commission, the Minister shall at all times ensure that the independence of the Commission, in regard to the discharge of its functions and operations under this Act, is protected and not compromised in any manner whatsoever.

Although the Communications Act seeks to protect the independence of the regulator, the NCC is not altogether independent of the influence of the government as hitherto exerted through the Ministry of Communications and then through the Ministry of Information and Communication. A new Ministry, the Ministry of Communications Technology was created in 2011 by the government of President Goodluck Jonathan, "to foster a knowledge-based economy and information society

[342] See n 322.

in Nigeria."[343] The NCC is listed as one of the agencies under the Ministry, thus the supervision of the Commission has been transferred to the new Ministry. The NCC's independence is diminished by the fact that it is still retained as a department of the Ministry of Communications Technology and is supervised by the Minister. Furthermore, the government controls the process of appointment of the Chairman, the Executive Vice Chairman and members of the Commission and thereby exercises significant influence over their stay in office. The principal officers of the Commission such as the Chairman, the Executive Vice Chairman and the Commissioners are appointed by the President on the recommendation of the Minister.

The observations made about the influence of the Ministry of Information and Communications on the independence of the NCC are also applicable to the new Ministry as it will exercise the functions hitherto performed by the Ministry of Information and Communications.

As part of its supervisory role in the industry and in response to the rapid technological developments in telecommunications, broadcasting and ICTs, the Ministry of Information and Communications started the process of consultations with a view to updating the *National Telecommunications Policy* (NTP) which was formulated in the year 2000. In August 2011, a report on the review of the policy was submitted to the Minister of Communications Technology which is now the supervising Ministry in charge of telecommunications. The Minister has indicated that after consultations with relevant stakeholders in the industry, a national ICT Policy will be released. The new policy will harmonise the policy directions in the telecommunications and IT policy documents.[344] The influence of the Ministry of Communications Technology in the regulation of the telecommunications industry, though tempered by the Communications Act, cannot be waived aside. The Minister in charge of the Ministry still exerts a measure of control over the Nigerian

343 See the Ministry's website [online].

344 Nweke 15th August 2011 *Daily Champion*.

Communications Commission and there have been insinuations of interference by the Minister in the matter of frequency allocation.[345]

4.2.3 The Nigerian Communications Commission

The Nigerian Communications Commission (NCC) is the statutory regulator of the telecommunications industry established by the *Nigerian Communications Commission Decree* No. 75 of 1992.[346] The Commission became operational in July 1993 and commenced full market liberalisation and sector reform in 2000. The main objectives of the Commission include:

- Creating a regulatory environment to facilitate the supply of telecommunication facilities and services;[347]
- Facilitating the entry of private entrepreneurs into the telecommunication market and the promotion of fair competition and efficient market conduct;
- Assignment and registration of radio spectrum to licensed operators.

---

345 In March 2010, the Federal High Court, Abuja, reversed the cancellation of the 2.3GHz licence issued by the Nigerian Communications Commission to Mobitel Ltd ("Mobitel") by Prof Dora Akunyili, the then Minister of Information and Communications. The judge quashed the Minister's directive on the ground that it was beyond her powers and thus null and void. He also ordered the Commission to release the frequency slot to Mobitel, an order to which NCC immediately complied. Mobitel had taken the Minister to court for cancelling NCC's licensing process which awarded the three 2.3GHz frequency slots to Mobitel, Spectranet, Multilinks and Telkom. See Muraina and Nkanga 19th March 2010 *Thisday*.

346 Now repealed by the Nigerian Communications Act, Laws of the Federation of Nigeria, 2003.

347 S 1 of the Communications Act, 2003 provides as follows:

The primary object of this Act is to create and provide a regulatory framework for the Nigerian communications industry and all matters related thereto and for that purpose and without detracting from the generality of the foregoing, specifically to –

(a) promote the implementation of the national communications or telecommunications policy as may from time to time be modified and amended;
(b) establish a regulatory framework for the Nigerian communications industry and for this purpose to create an effective, impartial and independent regulatory authority;
(c) promote the provision of modern, universal, efficient, reliable, affordable and easily accessible communications services and the widest range thereof throughout Nigeria;
(d) encourage local and foreign investments in the Nigerian communications industry and the introduction of innovative services and practices in the industry in accordance with international best practices and trends;
(e) ensure fair competition in all sectors of the Nigerian communications industry and also encourage participation of Nigerians in the ownership, control and management of communications companies and organisations;
(f) encourage the development of a communications manufacturing and supply sector within the Nigerian economy and also encourage effective research and development efforts by all communications industry practitioners;
(g) protect the rights and interest of service providers and consumers within Nigeria.

- Administration of national numbering plan;
- Establishing mechanisms for promoting universal access to telecommunication services nationwide;
- Enforcing technical standards and protection of consumers from unfair practices by licensees.

The Commission adopted a phased approach to the liberalization of the telecommunications sector by issuing a number of licences for telecommunications services, including licences for the provision of fixed line telephony services by private telecommunications operators. In the absence of a telecommunications policy to guide its activities however, the result of the Commission's early activities was not impressive. In 1998 the combined fixed telephone lines by NITEL and the PTOs was less than 450 000.[348] There was only one mobile cellular telephone network, provided by the Mobile Telecommunication Company Ltd (M-TEL), a subsidiary of NITEL. This poor state of the telecommunications industry prompted the formulation of the NTP in 2000.

The adoption of the Policy led to the enactment of the Nigerian Communications Act, 2003. In combination with the NTP, the Communications Act made extensive provisions for the regulation of the telecommunications industry. Issues such as licensing, general competition principles, investigations and appeals were addressed in the Act. Other areas include dispute resolution, interconnection, access to facilities, universal service, spectrum management, numbering and technical standards. To ensure the realisation of the objectives set out in the NTP and the Communications Act, the Act vested wide powers in the NCC and constituted it the main regulator of the industry in Nigeria.[349]

The Commission is empowered to make regulations exempting categories of services from licensing altogether.[350] Under section 4(f) of the NCC Act, the Commission is responsible for the promotion of competition in the industry. It is also responsible

---

348 International Telecommunication Union (ITU) *Licensing in the Era of Liberalization and Convergence: The Case Study of the Federal Republic of Nigeria* 8.

349 S 3 Nigerian Communications Act, Laws of the Federation of Nigeria, 2003.

350 Id at s 31and 32.

for protecting the providers of telecommunications services and infrastructure from unfair and anti-competitive practices.[351] The Commission has powers under section 70(1) of the Nigerian Communications Act[352] to make regulations for the guidance and direction of the industry. There is however, no provision in the said section for regulations that will secure the privacy of telecommunications and so no such regulations have been made by the Commission. It is pertinent to note that one of the objectives of the Act is to protect the rights and interests of service providers and consumers within Nigeria.[353]

Although no definition of "communications" is made in the Act, it is clear that the Act applies to "the provision and usage of all communications services and networks, in whole or in part within Nigeria or on ships or aircraft registered in Nigeria."[354] Telephone calls and e-mails form part of the communications services offered in Nigeria. In the opinion of this writer, the failure of the NCC to make regulations for securing the privacy of communications is a major weakness in the regulatory capability of the NCC.

This is all the more disturbing in the light of newspaper reports suggesting that the government has taken steps to intercept telephone conversations in the face of growing terrorist, religious and ethnic attacks in the country. According to a report in one of the local newspapers,

---

351 S 4(g) Nigerian Communications Commission Act, Laws of the Federation of Nigeria, 1992.

352 The Commission may publish regulations for any or all of the following matters:
(a) written authorisations, permits, assignments and licences granted or issued under the Act ;
(b) assignment of rights to the spectrum or numbers under Chapter VIII, including mechanisms for rate-based assignment ;
(c) any fees, charges, rates or fines to be imposed pursuant to or under the Act or its subsidiary legislation;
(d) a system of universal service provision under Chapter VII, including but not limited to the quality of service standards ;
(e) communications and related offences and penalties;
(f) any matter for which this Act makes express provision; and
(g) such other matters as are necessary for giving full effect to the provisions of this Act and for their due administration.

353 See n 349 at s 1(g).

354 Id s 2.

> [t]he federal government might have authorised the monitoring of telephone lines of persons suspected to be involved in activities that may jeopardise the nation's security. The directive, it was learnt was handed down to the Nigerian Communications Commission which regulates the activities of telecommunications operators in the country.[355]

The question that arises is whether the Nigerian Communications Commission, in the absence of internally formulated regulations for the protection of the privacy of users of communications networks, and in the absence of statutory safeguards against illegal access to private communications by governments and private persons and entities in Nigeria, is in a position to fulfil its statutory mandate to protect the interests of the providers and users of communications services in Nigeria as stipulated by the Communications Act.

Lawful interception is nothing strange; it is the means by which law enforcement agencies are permitted, under a specific law, to intercept the communications of persons under suspicion of a crime. However, the problem with lawful interception arises where there is an absence of safeguards against abuse of the government's right to access private communication. In the case of Nigeria, the absence of a statute requiring judicial oversight of governments' interception of communications raises the question whether there is any reasonable expectation of privacy in communications, notwithstanding the constitutional guarantee of the same.[356]

The argument that access to communications gives law enforcement agents a veritable tool to fight crimes, particularly terrorism, resonates well in a society where criminal and terrorist activities are on the increase as in Nigeria in recent times.[357] Nevertheless, there are concerns about interception of communications whether lawful or otherwise, that should be addressed. One such concern is the clear possibility of

---

355 Odittah and Isine 10th Oct 2011 *Leadership* newspaper.

356 S 37 of the Nigerian Constitution 1999 protects the privacy of communications. The question of privacy will be addressed in the next chapter.

357 The two primary threats to national security in Nigeria are violence in the Niger Delta and sectarian strife between Muslims and Christians in the northern part of the country. The violence in the Niger Delta is generally agreed to be due to the long neglect of the infrastructural deficiencies in the region and the environmental degradation occasioned by oil exploration activities. See Sunday 31st May 2009 *Sunday Trust*.

abuse of the right of interception. Even in countries with established traditions of respect for rule of law and the rights of the people, unlawful interference with citizens' communications are known to happen in clear violation of extant laws.[358]

Secondly, there is the question of trust. In the absence of safeguards, and even where such safeguards are available, it is debatable whether Nigerians trust their governments enough to believe that access to citizens' communications will be managed responsibly and without it being hijacked by particular interest groups such as the political class or any other group, as a weapon against political opponents or other persons adjudged by the state and its officials as "enemies of the state". What happened in Greece in 2004[359] during the Olympics Games, where unlawful intercepts of telephone communications was discovered, is a pointer to what can happen in a weak regulatory environment; it should not be allowed to happen in Nigeria. These concerns are weighty enough to compel a serious consideration of the need to adopt a data privacy law in Nigeria to safeguard information privacy, more so as the country's recent history suggests that democratic traditions and respect for rule of law are not yet fully entrenched. Nigeria needs to learn from the experiences of other countries with regard to addressing the issues of national security and information privacy. More will be said in chapter 7 about addressing the information privacy concerns of Nigerian citizens in an era of widespread use of telecommunications technologies and increasing security threats.

---

358 In the US, a federal judge ruled that the National Security Agency's program of surveillance without warrants was illegal and in violation of a 1978 federal statute which required court approval for domestic surveillance. According to a newspaper report, the National Security Agency monitored Americans' international e-mail messages and phone calls without court approval, even though the Foreign Intelligence Surveillance Act, or FISA, required warrants. See Savage and Risen 31st March 2010 *New York Times* [online].

359 During the 2004 Olympic Games in Greece, Vodafone's mobile phone operation in Greece was "embroiled in a phone-tapping scandal, nicknamed the Greek Watergate, after it discovered its network was being used to eavesdrop on the country's political and military elite." The telephone operator, Vodafone Greece was fined €76m for failing to secure its systems against unlawful access that led to illegal wiretapping. See Smith 7th February 2006 *The Guardian*.

4.2.4 Nigerian Telecommunication Limited (NITEL)

NITEL was the national operator and monopoly service provider for domestic and international services. The main objective of establishing NITEL was to harmonise the planning and co-ordination of the internal and external telecommunications services, rationalise investments in telecommunications development and provide accessible, efficient and affordable services. However, the slow pace of network rollout, non-competitive equipment procurement procedures and sub-optimal quality of service delivery, resulted in a weak infrastructure base that failed to meet the demands for telecommunication services.[360]

The release of a telecommunications policy in the year 2000 ushered in a new era of full liberalisation of the telecommunications industry. The implementation of the policy resulted in the successful auctioning of the 2G Digital Mobile Licenses in January 2001 with a total of four GSM licenses issued.[361] Furthermore, a number of Fixed Wireless Access (FWA) operators were licenced in 2002 (both national & regional licenses issued) and even more significantly, a Second National Carrier, Globacom was licensed in 2002. The incumbent operator, NITEL, was brought under the regulatory oversight of the NCC in 2000 and was formally licenced in 2001.[362] As part of the privatisation and commercialisation programme of the Nigerian government, NITEL has been on offer for sale since 2001. All the attempts made so far by the Bureau of Public Enterprises (BPE), the government agency responsible for the privatisation of government enterprises, to sell the company have failed to produce a credible buyer for the premier telecommunications company. In 2001, Investors International London Limited made the first attempt to acquire NITEL but failed to pay the bid price of $1.317 billion and thereby lost the attempted acquisition. Pentascope, a Dutch company, was thereafter appointed to manage the telecoms company but the arrangement was not without controversy. The management contract was eventually cancelled.

---

360 Ndukwe *Telecoms Regulatory Environment* 8 [online].

361 Id at 29.

362 See n 338 at 18.

In 2006, a consortium led by Transnational Corporation of Nigeria (Transcorp) won the bid to acquire a controlling 51% stake in NITEL. Due to Transcorp's inability to pay off NITEL's debts and invest in the operator's network, British Telecommunications (BT), a member of the consortium, pulled out of the management consortium in mid-2007, citing financing problems. In 2009, the government announced the revocation of the sale to Transcorp, on the ground that the buyer breached the shares sale agreement.

Following the revocation of the sale to Transcorp and the failure of the preferred bidder, New Generation Consortium, to meet payment deadlines, the BPE invited the reserve bidder Omen International to re-validate its interest in NITEL by making the necessary initial payments.[363] The BPE has indicated that it would explore other options for disposing of NITEL should the reserve bidder fail to pay.[364] The long delay in privatising NITEL has taken a heavy toll on its fixed assets which are not only deteriorating, but also diminishing in terms of subscribed lines. For example, MTel, the mobile subsidiary of NITEL, saw its share of the GSM market drop from 10.7% in 2001 to 0.4% in 2009.[365] NITEL's inability to operate maximally as a national carrier has negatively affected its ability to invest in necessary telecommunications infrastructure. This in turn accounts for its inability to provide adequate switching facilities for the new entrants into the industry to connect to, thereby compounding the interconnection challenges that have plagued the industry for many years.

4.2.5 The second national operator – Globacom Ltd

Globacom Limited is a wholly owned Nigerian company that was granted licence by the Nigerian Communications Commission as the second national telecommunications operator in 2003. As the second national telecommunications operator, the company is entitled to and does operate fixed line phone, mobile, internet and international gateway services. Glomobile, the cellular unit, was

363 See Nwankwo 3rd July 2011 *Leadership* newspaper.

364 Ibid.

365 Pyramid Research *The Impact of Mobile Services in Nigeria* 36 [online].

launched in August 2003 and quickly built up its subscribers to 1.9 million; by September 2010, the number of subscribers increased to 17.6 million. This phenomenal growth made it the fastest growing GSM network in Africa.[366]

Globacom made a significant impact on the telecommunications market upon its entry into the market in 2003. The company, through its mobile subsidiary Glomobile, introduced per second billing for calls and thereby launched true competition in the market. Another significant milestone of Globacom's entry into the market was the introduction of the one Naira SIM, thereby making the acquisition of mobile telephone lines affordable to almost every strata of Nigerian society.

Furthermore, the company rolled out its operations with superior and more up-to-date technology and thereby catalysed the technological development of the telecommunications industry by compelling the other networks to upgrade their network technologies and introduce value added services in the industry. In August 2006, Glomobile became the first network to launch and operate the Blackberry service in Nigeria. Also, Globacom is the only private indigenous telephone company in Nigeria to own and operate a submarine fibre optic cable which connects the West coast of Africa to the United Kingdom and through the UK to a hub in the US. The Glo-1 cable landed in Lagos, Nigeria in September 2009.[367] It was widely expected that the landing of the cable in Nigeria will translate into much faster and more robust connectivity for voice, data and video and boost economic activities in the region, create job opportunities and serve companies in Europe and Africa.[368] That expectation has not yet been realised.[369]

Although Globacom has made very impressive contributions to the growth of the industry since it commenced operations, it has, much like the other operators in the industry, not performed well in terms of the quality of its services and the consumer

366 NCC Report *Trends in Telecommunications Markets* 45 [online].

367 Ikoabasi 29th August 2011 *Daily Trust*.

368 Osuagwu 6th September 2009 *Vanguard*.

369 Okonedo and Uzor 3rd January 2012 *Businessday*.

complaints arising therefrom. There seems to be a widely held thinking on the part of the company and the other operators in the market, that what they fail to provide in terms of quality of service, they can always make up for by a ceaseless stream of promotional undertakings that promise to give away cars, gadgets and large sums of money.[370] The company needs to significantly reduce cases of dropped calls occasioned by network congestion.

Globacom, like all the other major PTOs, was perhaps overwhelmed by the very enthusiastic embrace of digital mobile telephony by a society starved of telecommunications services for a long time. For example, Glomobile recorded 1 million subscribers within 9 months of operations.[371] This impressive uptake of customer subscriptions happened at a time when it had not rolled out sufficient infrastructures to handle the surging number of customers and has had to play catch up since then just like the others. A natural consequence is the frequent congestion of networks and dropped calls that has characterised the operations of Globacom and the other operators in the market. In October 2011, the regulator, NCC, threatened to sanction the major GSM operators if they did not show a measurable level of improvement in the quality of their services. The regulator gave the companies a 30 days ultimatum to improve the quality of their services failing which each network will be banned from adding any new customer and fined 1 million naira per any new customer subscription added to the network.[372]

Another weak area of operation is that of customer care and the handling of consumer complaints. In the face of growing competition, the NCC set up a consumer's forum where consumers can air their grievances against any or all of the operators. None of the operators has seen it fit to establish their own interactive platforms for dealing with the complaints of their customers. The capacity of the

370 Giginyu 3rd January 2012 *Daily Trust.*

371 An ITU case study of Nigeria's telecommunications industry in 2004 noted that the roll-out targets for each of the licenced mobile operators' was 100,000 lines within 12 months of launching operations, 750,000 lines within 36 months and 1,200,000 within 60 months. Each of the operators exceeded its first target within a few months of launching service. By mid-2004 less than 2.5 years from first launch the four operators had, a total of over 5 million subscribers. See Moshiro *Licensing in the Era of Liberalization and Convergence* 16 [online].

372 See Adaramola 26th October 2011 *Daily Trust.*

operators for receiving feedback directly from customers other than what the regulator forwards to them for action, is seriously undermined. It is curious that Glomobile's customer care service for example, is almost completely offline notwithstanding the broadband capacity of the company. The result is that the customer care centres are usually overcrowded and unnecessary man-hours are lost by customers who have to queue up to be attended to in respect of some complaints that could very easily have been resolved online. Migrating key aspects of their customer care service to the Internet will reduce the number of customers waiting in the customers care offices of the company.

4.2.6 Other licensed private telecommunication operators and service providers

The deregulation of the telecommunications industry in 1993 opened up the market to private telephone operators who were granted licences to operate limited mobile and fixed wireless services. Between 2001 and 2004, a total of 523 new telecommunication licences had been issued by the Nigerian Communications Commission. There are about 30 active fixed and mobile operators and at least 80 Internet Service Providers (ISPs), many of them using Very Small Aperture Terminal (VSAT) satellite equipment across the country.[373]

The major private telephone operators[374] in the industry and their subscribers as at June 2011 are:

GSM (Global System for Mobile Communications) Technology

MTN Nigeria	40,540,281
Airtel	15,969,943
MTEL	258,520
Etisalat	7,835,673
Glo	19,488,756

CDMA (Code Division Multiple Access) Technology

[373] NCC *Operator Quarterly Summary* [online].

[374] Ibid.

Starcomms	1,154,837
Visafone	2,596,401
Multilinks	974,076
Reliance Telecoms (Zoom)	833,298

While the deregulation of the telecommunications market, which witnessed the licensing of several small and medium sized operators in Nigeria, has been largely successful, the multiplicity of operators in the sector poses a number of challenges. The lack of adequate telecommunications infrastructures has been a significant constraint to the new entrants. The inability of the former monopoly operator NITEL, to provide adequate backbone infrastructure facilities for the new operators to connect to, resulted in the PTOs having to install their own infrastructures, thereby diverting investment that could have been used for rolling out their services. This in turn accounts for the congestion in network traffic that has diminished the quality of service of all the operators in the industry.

The observations made about Globacom above apply also to the PTOs in regard to their service delivery and customer care delivery. Furthermore, a key enabling factor for effective ICT infrastructure deployment is reliable and adequate supply of electricity. The unreliable power supply in Nigeria has compelled the telephone companies to generate their own power supply to keep the GSM and fixed-line networks running. The resort to generators and the diesel to run them, increases the cost of operations by the companies and partly accounts for the continued high tariffs in the industry. The NCC, while acknowledging that erratic power supply contributes to the poor quality services rendered by the operators, notes also, other factors such as vandalisation of telecommunications infrastructures, insecurity and multiple taxation, as contributing to the challenges facing all the PTOs in the industry.[375]

[375] In a recent newspaper report, the Executive Vice-Chairman of the Commission said:

> We are not unaware of the challenges which such rapid growth has visited on the industry. The good news is that the NCC is providing regulatory intervention to curtail such challenges. The main challenge has been that of QoS which has not reached the envisaged level of efficiency. Erratic public power supply, vandalisation of telecoms infrastructure, lack of basic infrastructure, high level of insecurity, multiple taxation all collectively affect expected performance from the industry. See Uzor 3rd January 2012 *Businessday* newspaper.

4.2.7 National Frequency Management Council (NFMC)

The new Nigerian Communications Act, 2003 provides for the establishment of the National Frequency Management Council (NFMC)[376] under the Ministry of Information and Communications, with the Minister designated as chairman. It is responsible for the planning, co-ordination and bulk allocation of the radio frequency spectrum in the country. The Council must liaise with the Nigerian Communications Commission (NCC) and the Nigerian Broadcasting Commission (NBC) on the assignment of frequencies.

The functions of the NFMC include the following:

- Enforcing rules and regulations for the effective utilisation of the frequency spectrum on the basis of national priorities;
- Identifying the spectrum requirements to satisfy the needs of the country;
- Producing a National Frequency Plan and allocating bulk frequency ranges to regulatory bodies (NCC and NBC) and relevant government agencies. The National Frequency Plan shall identify ranges of frequencies to be made available for telecommunications and broadcast services. However, the actual assignment of specific frequencies within these ranges to licensed operators shall be the responsibility of the NCC and the NBC.[377]

The NCC appears to be the most dominant regulator of spectrum allocation due in part to the significantly larger market size of the telecommunications industry vis-à-vis broadcasting. The Commission's dominant position in the development of frequency spectrum policies and allocation of spectrum is further boosted by the fact that the contribution of the telecommunications industry to the national GDP has been steadily growing since 2001 when it contributed a mere 0.62% to GDP. In 2009, the industry's contribution to GDP stood at 3.66%.[378] In 2010, the contribution of the

376 See s 26 Nigerian Communications Act, Laws of the Federation of Nigeria, 2003.

377 Id s 28.

378 See NCC website [online].

industry was put at 8.2 per cent, while those of manufacturing, banking and solid minerals were 3%, 4% and 0.4% respectively.[379]

The country has been divided into licensing areas, comprising the 36 states and Federal Capital Territory (FCT), for the purpose of frequency licensing. Spectrum fees vary from state to state according to the market potentials and level of economic activities in the licensing area. The 37 licensing areas of the federation have been categorized into five tiers, with "tier 1" having only Lagos State, the commercial capital of Nigeria, as the most expensive, and the others in descending order.[380]

Globally, radio frequencies are regarded as scare national resources and managed with a view to maximising economic benefits from the allocation of the frequencies. Nigeria is not an exception. While it has generally managed frequency allocations without much ado, it appears to have struck a wrong chord in the allocation of the 2.3GHz frequency which had to be settled in court.[381]

5. REGULATORY FRAMEWORK

5.1 Introduction

A seminar in 1987 on restructuring the telecommunications sector in Nigeria, led to the first *National Telecommunications Policy* (NTP),[382] which has the following core objectives:

- Privatisation of the public monopoly, NITEL.
- Deregulation/liberalisation of the industry.
- Establishment of the National Regulatory Authority.

The overriding objective of the NTP is to achieve the modernisation and rapid

379 Tagbo 17th February 2011 *Businessday*.

380 See NCC website [online] for information on spectrum fees and pricing.

381 See n 345.

382 Ndukwe *Country Experience in Telecom Market Reforms – Nigeria* 26 [online]. In 1998 the Ministry of Communications published the maiden edition of the National Policy on Telecommunications. Upon assumption of office in 1999, the civilian administration of Chief Olusegun Obasanjo revised and published the Policy in 2000.

expansion of the telecommunications network and services in order to enhance Nigeria's development. It also aims to integrate Nigeria internally as well as into the global telecommunications environment.[383] In order to accomplish the NTP's objectives, the Nigerian Communications Act, 2003[384] established the Nigerian Communications Commission (NCC) and gave it the role of an independent regulator vested with all the powers previously exercised by the Minister of Communications under the Wireless Telegraphy Act, 1961.

5.2 Regulation and competition

5.2.1 Objectives of the regulatory framework

The primary objective of the regulatory framework is the promotion of competition, particularly in service provision, in the industry. Telecommunications policy and regulation need to foster effective and efficient competition, while also recognising social policy goals of making the service universally available and affordable.[385] Furthermore, the ultimate purpose of a good regulatory agency is to protect consumer rights and interests, as is the case in countries where there is open competition in telecommunications services. The NCC acknowledges that maintaining a transparent regulatory regime that protects the consumer is one of its key roles in the telecommunications industry.[386] Opening up the telecommunications industry to keen competition is the pragmatic thing to do in the light of the economic imperatives. The high financial capital outlays required for deploying the latest, cutting-edge telecommunications technologies are simply not affordable by the Nigerian financial system without outside help.

The licensing of Globacom Limited as the second national operator accomplished one of the NTP's objectives of having at least two fixed-line service providers. NITEL, the dominant operator, cannot meet the needs of all prospective users. The NTP, along with the establishment of the NCC as the national regulatory agency, signalled

383 See n 313 at Ch 2.

384 The Act came into force in July 2003; the Nigerian Communications Commission had been set up by the Nigerian Communications Commission Act, 1992 (now repealed by the Communications Act, 2003).

385 See n 367.

386 Ndukwe *NCC Policy and Strategic Thrust – 2005 and Beyond* 19 [online].

Nigeria's transition from a monopoly regime to a competitive one.[387] In order for this transition to be effective however, Grewlich cautions that:

> As telecommunication migrates from monopoly to competition, government has the crucial role of being a neutral force in the economy that must ensure a minimum-interventionist pro-competitive regulatory framework with transparent rules and value to the user.[388]

Nevertheless, two major and interrelated regulatory issues that the government and the NCC have to deal with are interconnection and convergence.

5.2.2 Interconnection

The seamless interconnection of new and existing operators in the telecommunications industry is vital to the successful implementation of a competitive telecommunication market. Without an effective interconnection regime and seamless communications between consumers on different networks, the value of the network to customers is very limited.[389] The ability of newly licensed operators to interconnect with the dominant operator's network is a fundamental requirement which needs careful regulation in order to avoid distortions in the system. One of the complaints against NITEL, the former monopoly backbone operator, is its unwillingness or inability to effect interconnection of other operators to its network; NITEL is however not the only operator blamed for constraining interconnection.[390] The legislative framework for effecting interconnectivity is section 96 of the *NCC Act*.[391] The Act makes interconnection between network services or facilities mandatory and declares that the terms and conditions of interconnection agreements

---

387 See n 316.

388 Grewlich *Governance in 'Cyberspace': Access and Public Interest in Global Communications* 93.

389 Esselaar, Gillwald and Stork *Towards an African e-Index 2007* 41 [online].

390 Interconnection disputes continue to disrupt telecommunications services in Nigeria and NITEL is not the only culprit. In April 2004, the NCC imposed a fine of 34 million naira (Nigerian currency) on Globacom, the second national operator, for failure to interconnect smaller private telecommunications operators even after a direction to do so was given by the Commission. See NCC *Headlines* [online].

391 The NCC was initially established under the old Nigerian Communications Commission Decree No 75 of 1992 now repealed by the Nigerian Communications Act, 2003. S17 (1) of Decree No 75 granted a right to a licensee or authorised carrier to interconnect his network facilities to the network of another authorised carrier.

are primarily to be agreed upon by the operators. The Commission is empowered to intervene and make binding determinations at the request of either or both parties to interconnection negotiations.

The interconnection conflicts in the telecommunications industry have, in the past, been primarily between NITEL, the former dominant operator and the PTOs licenced by the NCC. The increased number of licenced operators further compounded the problem of connectivity as they all had to rely on NITEL, the only national carrier and provider of backbone services before Globacom was licenced as such. These conflicts with NITEL were mostly caused by the inability of the parties to agree on interconnection rates or failure to pay the interconnection fees demanded by NITEL. In the period before 2003, the conflicts were moderated by the then Ministry of Communications which did not have the will or capacity to call NITEL to order. The NCC also did not at this time have the necessary statutory power to regulate NITEL.

Prior to 2003 when the Nigerian Communications Act was enacted and the NCC established as the main regulator of the industry, NITEL, the former monopoly telecommunications provider, was not under the regulatory control of the NCC. The NCC was essentially a department under the then Ministry of Communications just as NITEL was and could not exercise effective regulatory control over the government monopoly telecommunications company. The situation changed however when the Communications Act was enacted and NCC was given wide regulatory powers over all players in the industry.

In 2003, after NITEL came under the regulatory supervision of the NCC, the Commission intervened in the interconnection disputes by convening a meeting between all the players in the industry to resolve the conflict. The outcome of the meeting was the adoption of a revised interconnection rate agreement which most of the operators agreed to with the exception of Mobile Telecommunications Network (MTN), one of the GSM operators, which opted to challenge the competence of the Commission to impose the agreement on it in court.

The process of achieving interconnectivity differs from country to country.[392] While judicial action has been the major path of expansion in the US and EU, Nigeria has largely adopted a muted negotiation route which has often been held up by bureaucracy and the intransigence of the key operators.[393] With the addition of more investors in the industry as a result of the successful auction of 4 2G GSM licenses in February 2001 and 4 3G licenses in 2007, it was expected that recourse to litigation to enforce interconnection rights would be a viable option in addition to NCC's regulatory intervention. In the case of litigation, the Federal High Court will be called upon to exercise jurisdiction in determining such disputes.[394]

Not much has happened by way of litigation in resolving interconnection disputes, but a news item in one of the local newspapers suggests that the operators are not averse to litigation for the settlement of their interconnection disputes.[395] It is however the responsibility of the NCC to ensure that interconnection is available on a non-discriminatory and cost-oriented basis to all licensed operators by drawing up a transparent set of interconnection rules, which shall be published and made available to all operators in the industry.[396]

Although much credit has been given to the NCC for its management of the deregulation of the telecommunications industry in Nigeria in the last decade, the Commission's strategy of mixing deregulation with sometimes opaque intervention has not always met the needs of the industry. One area of such intervention is the vexed issue of interconnection between the operators. In a review of African trends in

---

392 In Nigeria, the process is mostly by negotiation between the two national operators with backbone capacity, NITEL and Globacom, and the new private telecommunications operators, supervised by the NCC. In the US, the process has been predominantly through private litigations against Telco giants like AT &T and MCI WorldCom; (*US v AT&T* 524 F Supp 1336 (DC C) 1981); *MCI v AT&T* 708 F 2d 1081 7th Cir). The process of liberalisation in EU has been accomplished by careful implementation of the EU Treaty provisions for free movement of goods and services, through infringement actions such as *Italy v Commission* (1985) ECR 873; see Stahl 1994 (19) *Yale J Int'l L* 405.

393 Ibid.

394 S 138 Nigerian Communications Act, 2003.

395 *Vanguard newspaper* 14 January 2010 [online].

396 A telecommunications networks interconnection regulations document was released in May 2003 by the NCC pursuant to s 97(B) of the Nigerian Communications Act, 2003. See NCC *Telecommunications Networks Interconnection Regulations* 2003 [online].

investment and competition in the telecommunications industry in 16 African countries including Nigeria and South Africa, the report, while generally applauding Nigeria's good performance in other areas of the review, observed, in relation to interconnectivity, that "[t]his vital area of competition is the one area where Nigeria scores negatively."[397]

According to the report, the negative perception in this area of NCC's regulation may have resulted from:

> ... the commitment in the guidelines by NCC, to limit the extent of the obligations of the dominant operators during the period of transition to full competition at the exact point when new entrants most require assistance and for favourable conditions to default in their favour.[398]

The failure of the Commission to name the dominant operators in the market ten years after deregulation is one reason why NCC-led negotiations on interconnection charges have always generated controversy and failed to either satisfy all the stakeholders in the industry or bring down telephone tariffs in Nigeria.[399]

5.2.3 Convergence

Convergence entails the coming together of content (from the audio-visual and publishing industries), infrastructures (such as those supporting telecommunications services or broadcast television) and the processing and storage capabilities of computers and consumer electronics servers and terminals.[400] The impact of the new services resulting from convergence will be felt throughout the economy generally

---

397 See n 389 at 42.

398 Ibid n 389.

399 Ibid n 391. See also Abayomi 12th June 2010 *Daily Independent*.

400 The EU Commission, in its *Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications of Regulation - Towards an Information Society Approach* ii, recognises that convergence, pertaining to telecommunications, information technology and broadcasting, is occurring at the technological level such that digital technology now allows both traditional and new communication services whether voice, data, sound or picture, to be provided over many different networks.

and in the respective sectors particularly.[401] There is growing awareness in the industry that the convergence of technologies presents new challenges to the national regulatory authority; for example, in a communiqué issued at the end of a two-day gathering of telecom stakeholders in Abuja, Nigeria, the participants noted that:

> There is rapidly growing Technology Convergence which is blurring the traditional boundaries between telecom, datacom and Video/Broadcasting. Convergence is therefore upon us - leading to unified data, voice, video and multimedia communications; and poses a new set of regulatory challenge such as the case with Voice over Internet Protocol (VoIP).[402]

One of the key challenges that the convergence of technologies presents to the regulatory authority is the protection of data that users send and receive across the converged technologies. The main focus of data protection is the regulation of data relating to the individual. Data protection is a major challenge because its absence will no doubt impact the way the public uses the telecommunications networks. If users of telecommunication facilities become doubtful of the privacy of their communications, they will refrain from further use of such facilities. The chilling effect this can have on the industry and indeed the whole economy makes it a regulatory matter the government should be involved with.

---

401 In 1998, the Wireless Telegraphy Amendment Decree No 31, 1998 amended the Act. The explanatory note to the Decree states that:

> The Decree amends the Wireless Telegraphy Act to modify provisions, which inhibits competition in the communications sector. Accordingly, the Decree amongst other things defines the role of the Nigerian Communications Commission and the National Broadcasting Commission which under the Decree establishing them, are responsible for matters relating to telecommunications and broadcasting respectively, as contained in the Act.

As the law stands today, and in view of the global phenomena of convergence, there is room for conflict between the NCC and the Nigerian Broadcasting Commission, both of which are empowered to issue licenses for operators needing a piece of the Nigerian spectrum. There is need to streamline the regulatory framework for spectrum allocation so that while one statutory organ is responsible for allocation, the other can be in charge of maintaining standards as is the case in Singapore where the IDA Act (No 41 of 1999) provides for the formation of the Info-communications Development Authority of Singapore ("IDA"), which is a merger of the National Computer Board ("NCB") and the Telecommunication Authority of Singapore ("TAS"). The IDA Act sets out the powers, functions and duties of IDA as the regulator and promoter of information and communications technology; the Singapore Broadcasting Authority regulates broadcast and Internet content.

402 Ajakaye 16th Nov 2005 *Thisday* newspaper.

5.3 National policy on telecommunications

The *National Policy on Telecommunications* (NTP) recognises the global trend in telecommunication policies that integrate the advantages of rapid technological developments in telecommunications, broadcasting, and information and communication technologies (convergence). It therefore envisages that Nigerian communication laws will be reviewed and made more all-encompassing in line with the international best practices, towards convergence of technological and market forces in the communications and information technology.[403]

Because the Internet is essentially a communications technology much like the telephone and other such devices, the NTP recognises that access to the Internet falls under telecommunications services offered in Nigeria.[404] However, the Communications Act does not prescribe any specific rules regarding access to and use of the Internet.[405]

At the core of the NTP and Communications Act, 2003, lies the need to attract investment to develop the national ICT infrastructure. This has resulted in policy and institutional reforms.[406] Telecommunications being the backbone infrastructure of the emerging global information society, Nigeria's challenge is to rapidly expand its telecommunications and information technology base as a vehicle for sustainable economic development. It is recognised that without a solid telecommunications and information infrastructure, the country will not attract the right level of urgently needed local and foreign investment to build the economy.

---

403 Chp 3.2 *National Policy on Telecommunications*, 2000.

404 Id at chp 1.2.1(xix).

405 In April 2013, the *Premium Times*, a Nigerian newspaper, carried a report that the Nigerian government had entered into a secret agreement worth $40million, with an Israeli company to monitor computer and Internet communications by Nigerians. Although the report has been denied by government officials, it is very unlikely, given the extent of details disclosed in the newspaper report that, government's denial will persuade any careful observer of the deteriorating security situation in Nigeria and the pressures being exerted thereby on the government to take a firm control of the situation to the contrary. The implication of this report is that if true, Nigeria will join the ranks of nations such as China, Iran, etc, that monitor and restrict access to the Internet. See Ogala April 25, 2013 *Premium Times*.

406 Ndukwe *Nigerian Telecommunications Environment* [online].

5.4 The national regulatory agencies: failure to protect information privacy

5.4.1 Nigerian Communications Commission (NCC)

The Nigerian Communication Commission is expected to accomplish the objectives set by the NTP by:

- Extending availability of Telecommunications Services to all Nigerians;
- Promoting effective competition in the market, to ensure fair pricing of good quality telecommunications services;
- Protecting consumer rights and interests;
- Encouraging massive investment in the Telecommunications Sector;
- Encouraging new and advanced services.[407]

In carrying out its mission, the NCC has identified the consumer as the major focus of its activities; the goal is to ensure customers' satisfaction with the services provided by the telecommunications companies. While the NCC acknowledges that it has a number of challenges to surmount in fulfilling its mandate, it does not appear that privacy (or data protection) lies at the top of its priority list. The regulatory regime that the NCC presides over has thus far concentrated mainly on issues revolving around infrastructural deficiencies. Emphasis on the technical domain is understandable as it assures quality service delivery by the telecommunications and network service providers under the regulatory supervision of the NCC. Even so, the Commission is yet to address issues such as encryption, anonymisers, cookies and spyware.

It is necessary for the Commission to recognise that a number of the actions or activities undertaken in the technical domain, crossover into the social domain of telecommunications. This social aspect also needs to be adequately regulated in order to safeguard the privacy of users and protect the integrity of data coursing through the technical infrastructures. Because of the increased amount of personal information available at large either through the use of the Internet or by simply making a phone call, the privacy and security of telecommunications is increasingly under threat from the very technologies that make communication possible. For

[407] See n 403 at chp 3.1.4.

example, a study done for the Electronic Privacy Information Center (EPIC) on the impact of mobile technology on location privacy, identified three distinct but discrete operations as needed for transforming raw data captured by mobile devices such as cellular phones, into personal information.[408] First, there is the initial gathering of transaction-generated data; secondly, the data is processed to transform it into useful information; and thirdly the resultant information is applied, either to enhance commerce as is prevalent in the US, or simply for public use.

The whole process of transforming raw transaction-generated data into personally identifiable information raises information privacy concerns in four distinct phases: (i) in the initial collection of personal information; (ii) in the subsequent use of the information; (iii) in the disclosure of the information, and (iv) in the preservation and retention of the information. In all of these phases of telecommunications transactions in Nigeria, there is a glaring lack of protection for the privacy of personal data that is generated in the course of a telephone conversation. The recent directive by the government of Nigeria through the NCC that all SIM cards in Nigeria be registered and personal information of the owners/users collected, highlights this failure of privacy protection.

5.4.1.1 The privacy implications of SIM card registration

In March 2011, the NCC commenced the registration of all SIM cards in Nigeria. According to the Commission, the idea for the registration was first mooted in 2008 when security agencies approached the Commission for assistance in resolving crimes committed with the help of phones belonging to criminal elements that could not be identified with the numbers of the phones used in the crimes.[409] The objectives of the registration exercise are:

- To assist security agencies in resolving crimes and by extension to enhance the security of the state.
- To facilitate the collation of data by the Commission about phone usage in Nigeria.
- To enable operators to have a predictable profile about the users in their

[408] White *People, Not Places* 1 [online].

[409] See NCC *SIM Registration* [online].

networks.

- To enable the commission to effectively implement other value added services like Number Portability among others.

The registration of existing SIM cards, which was expected to be completed by September 28, 2011, officially ended in January 2012. The phone companies will however continue to register new SIM cards while all unregistered SIM cards would be disconnected from the networks.

In the face of rising criminal activities such as kidnappings, money laundering, terrorism, *et cetera*, the primary objective of registering all mobile SIM card owners/users is to capture the identity of the pre-paid mobile phone users who, before now, could purchase the Subscriber Identification Module (SIM) card anonymously. This element of anonymity is seen as giving criminal elements in the society the cover to engage in their criminal activities with impunity. Increasing concerns about the use of anonymous prepaid phone services for criminal and terrorist activities have persuaded several countries to introduce regulations requiring the registration of mobile phone users, particularly of customers using the prepaid services. Having all users of mobile phone services registered, the argument goes, will curtail those mobile phone assisted crimes and offer assistance to the law enforcement and security agencies in their pursuit of such criminals.

However, there are two major privacy right issues arising from the mandatory registration of mobile phone SIM cards that are not addressed by the NCC or the Nigerian legislature. The first issue is location privacy; the fact that a wide range of new generation mobile phones are equipped with global positioning systems capable of linking with global positioning satellites (GPS), makes it easy to track a mobile phone user's geographical location and movement with or without his knowledge, by using GPS or triangulation of GSM phone signal and base station locations.[410] Where the tracking is done without his knowledge, his privacy rights can be compromised

[410] See BBC News"Tracking a suspect by mobile phone" [online].

by the terms and conditions, under which the tracking, storage, processing and disclosure of the information generated to third parties, are handled.[411]

Unsupervised access to location information may cause "collateral damage" by revealing the kind of information that an individual wants and reasonably expects to be private. Examples are, information relating to a person's sexual orientation or associations, extra-marital liaisons, health history such as drug or alcohol abuse/treatment, information about the person's financial difficulties or transactions, domestic difficulties and other family matters (such as marital or family counseling, or the physical or mental health of one's children) and other matters of a potentially sensitive and extremely personal nature. These are matters that are capable of being disclosed as a consequence of unfettered access to a phone user's location information.

Furthermore, it raises the question of safety arising from accidental or unintentional sharing of location data that may result in annoyance, embarrassment or danger to the phone owner/user's safety. The issue of safety is particularly important because geo-location data can become dangerous information in the wrong hands. Thieves or stalkers with knowledge of an individual's present or future location can use this data to directly harm the individual and/or his property. The truth is, not every mobile phone user wants his co-workers, neighbours or even family to know where he is at every given point in time. In some cases, the revelation of this information could lead to embarrassment or even the loss of a job or a relationship. Apart from raising questions about who is collecting the location data, how it is used, with whom it can be shared with and how long it can be stored, it also raises questions about spamming by mobile e-commerce advertisers who can send unsolicited sms messages to mobile phone users.[412]

---

411 See however, s 12 Advance Fee Fraud and other Fraud Related Offences Act, 2006, which requires users of Internet services either at home or through Internet cafes to provide their full names and residential addresses to the Internet service provider or GSM service provider.

412 Mobile e-commerce is in its infancy in Nigeria and so the impact of mobile advertising may not be as significant as in the US. Nevertheless, e-spamming through mobile phones is already in operation in the urban centres of Nigeria and will continue to grow as more businesses realise the potential in mobile advertising.

The second issue is where a pre-paid customer may desire to withhold personal information from the mobile operator but is otherwise compelled to do so either at the point of purchase or at the point of activation of service as in the case of the SIM card registration in Nigeria. In this case, the privacy right issues also concern the terms and conditions under which the required personal information from the customer is collected, processed, stored and used by the phone company or regulator as the case may be. According to Gow,[413] SIM card registration raises the question whether there should be an entitlement to anonymity in the ownership and use of a telephone. The legal implications of SIM card registration, as affecting phone users' privacy rights, would perhaps have been better clarified if the NCC had opted to hold public hearings open to the public at large and not just selected stakeholders in the industry.

Gow argues that while it may be true that prepaid mobile phones are a chosen communications device for criminals and terrorists, it is not necessarily true that registration of prepaid mobile phones will act as a deterrent to those who are serious about committing criminal or terrorist acts.[414] He argues further that there is a persistent and often unexamined set of logical fallacies, or pitfalls, that tend to pervade policy analysis on the pre-paid customer's anonymity. For example, against the objectives set out by the NCC for requiring SIM card registration, it can be argued that factors such as loss or theft of mobile phones, roaming of mobile lines by tourists, business executives and traveling mobile phone users can compromise the accuracy of any phone database and thereby render the objective unrealisable or at best ineffective.

There are technologies available today that enable SIM card cloning whereby information contained in one SIM card is replicated in another phone for the purpose of making fraudulent calls. The bill for the fraudulent call would be incurred by the owner of the cloned SIM card rather than the perpetrator. To achieve cloning, the Electronic Serial Number (ESN) and Mobile Identification Number (MIN) have to be successfully retrieved from the target phone for transfer to the cloned phone. When this happens, calls can be made from the cloned phone as if it were originating

413 Gow 2005 *Convergence* 12.

414 Gow *Improving Identity Check Processes* 13 [online].

from the original phone.[415] Also, the availability of free Internet-based Voice over Internet Protocol (VOIP) services such as Skype, coupled with the use of satellite phones, all combine to circumvent the objectives of the NCC in requiring the collection of personal information at the point of purchase of mobile phones.[416]

From a national security perspective, the collection of personal information by the phone companies which are participating in the SIM card registration exercise raises information security concerns. One of the companies, MTN, a South African company, is the largest mobile phone company in Nigeria. The company has access to the personal data of over 40million Nigerians which are stored in Nigeria but readily accessible to the company's head office in South Africa. The volume of personal data MTN controls is more than any Nigerian government agency has in its database and one wonders if, in the absence of a data protection law, it is wise to allow such data in the custody of a foreign company. This theme will be further explored in chapter 6 when discussing the threats posed to national security by the trans-border flow of information generally and personal information in particular.

The NCC should realise that the issue, as far as the SIM card registration is concerned, is not whether the government can and should obtain the identity and movement/location information of suspect phone users, but that such information must be obtained by due process that meets the statutory standard set for such disclosure and approved by an impartial arbiter, the court. Unfortunately, that standard has not yet been set.

It will be useful to learn from the experiences of other countries. For example, in February 2008, the US government applied to a federal district court in the Western District of Pennsylvania requesting historical cell site location information for a particular person's phone number (i.e., information about what cell phone tower and what sector of the tower was receiving signals from the phone at a given time). The government argued that it can access this information merely by showing that the information is "relevant and material to an on-going criminal investigation" — a

[415] See Oruame 23rd June 2011 *The Nation*. SIM cloning was easier with older models of cell phones and though it can still be technically done today, there is no guarantee of successfully completing a cloning particularly for 3G SIM cards which are protected by anti-tamper software.

[416] Ibid.

standard lower than that usually required for search warrants by the Fourth Amendment.

In an extensive opinion, the presiding Magistrate Judge Lisa Pupo Lenihan denied the application, holding that the Stored Communications Act (SCA) does not authorize the government to obtain cell phone location information under the "relevant and material" standard, and that warrantless access to this information may violate the cell phone user's Fourth Amendment rights. On appeal, the US Court of Appeals for the 3rd Circuit disagreed with the lower court order and remanded it back to the magistrate judge for further hearing. The Appeal court however agreed that the SCA gives judges the discretion to require a warrant when the government seeks historical cell phone location information. The court also agreed that cell phone users have not given up their Fourth Amendment right to privacy just because their location information is shared with a third party, i.e., their cell phone provider.[417]

Nigerians have eagerly adopted mobile phone technologies with all the attendant risks they pose to information and location privacy. The NCC and the government of Nigeria should bear in mind however, that mobile phone users in Nigeria have not thereby given up their right to information privacy as guaranteed by the Constitution. The need to obtain information in order to fight crime must be carefully balanced against the need to also protect the privacy of phone users.

5.4.2 National Information Technology Development Agency (NITDA)

The National Information Technology Development Agency (NITDA) was established in 2001 to implement the National Information Technology (IT) Policy.[418] Some of the goals of the Agency include:

- To ensure that IT resources are readily available to promote efficient national development;
- To encourage local production and manufacture of IT components in a

[417] See US Magistrate Judge's denial of the Government's application under 18 USC 5 2703(d) to obtain cell site location information, *In the Matter of the Application of the USA for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government* [online].

[418] NITDA *The History of NITDA* [online].

competitive manner;

- To improve accessibility to public administration for all citizens, bringing transparency to government processes;
- To establish and develop IT infrastructure and maximise its use nationwide;
- To improve judicial procedures and enhance the dispensation of justice;
- To establish adequate institutional framework at the federal, state and local government levels in order to effectively accomplish the objectives of the IT vision and mission.[419]

To achieve these goals, the NITDA "... shall promote and guarantee freedom and rights to information and its use, protect individual privacy and secure justice for all by passing relevant Bills and Acts."[420] It will also "enhance freedom and access to digital information at all levels while protecting personal privacy."[421] To date, no data protection law has been enacted and the privacy guarantee in the constitution remains of doubtful utility in the drive to make Nigeria an IT hub in Africa.

5.5 A critical assessment of the regulatory framework

5.5.1 Introduction

The technical ability of the telecommunications and network service providers in Nigeria to gather, process, use, distribute and retain personal information has not yet come under the regulatory scrutiny of the NCC and other components of the regulatory infrastructure. Thus far, no regulatory guidelines or rules have been issued by the NCC to address these issues even though it recognises that security and privacy are essentials for securing customer protection and satisfaction.[422] Section 4(b) of the *Telecommunications Networks Interconnection Regulations* 2003, issued by the NCC, provides:

---

419 NITDA *National Policy for Information Technology* iii [online].

420 Id at 32. The NITDA is only mandated to sponsor Bills and Acts before the National Assembly.

421 Ibid.

422 See n 406.

> The Commission may impose conditions in interconnection agreements in order to ensure the protection of data, to the extent necessary to ensure compliance with relevant and regulatory provisions on the protection of data, including protection of personal data, the confidentiality of information processed, transmitted or stored and the protection of privacy.[423]

It is not known if the NCC has imposed such conditions or not; if it has, they are not known to the public and therefore remain of dubious utility to the consumers of telecommunication services. The interconnection agreements are the private documents of the telecommunications companies involved and none has yet published such an agreement. It is clear, however, that the primary duty to protect communication data and information privacy lies with the regulatory authority working in concert with the government.

5.5.2 Addressing the data protection policy problem

According to Bennett,[424] two principal and common elements gave birth to, and shaped information privacy protection policy in the post-industrial societies such as US, Germany, UK, Sweden etcetera. These elements are bureaucracy and information technology; these have created changes in the ways that public and private organisations collect and use personal information. It is these changes that prompted fears about "the implications for the personal privacy of citizens…" thereby giving birth to data protection/information privacy policies in those countries.[425]

In the countries where they are available, data protection policies and legislation arose as a consequence of technological development. The question arises therefore, whether the spread of ICTs in Nigeria is wide enough to create a critical mass sufficient to constitute technological development and thus elicit a data protection policy response from the government. The answer is clearly that Nigeria is still at the

---

423 Telecommunications Networks Interconnection Regulations 2003 available online at the NCC website .

424 Bennett *Regulating Privacy*.

425 Ibid at 2-3.

nascent stage of technological development. Nevertheless, the government's response to data protection issues so far has been an articulation of policy objectives in key policy documents but no commensurate legislative and/or regulatory response. For example, the *National Telecommunications Policy* declares that:

> Government shall continue to closely monitor the emerging applications of the Internet in areas such as banking, telephony as well as e-commerce and enact appropriate legislation and incentives that will encourage their use to promote rapid socio-economic development.[426]

The government is mindful of the benefits derivable from harnessing the potentials of ICTs in pursuit of the goal of socio-economic development. A Presidential Committee on Capacity Building for Outsourcing estimated in 2005 that Nigeria can earn about eight billion dollars annually from off-shore out-sourcing of ICT based services rendered to foreign based multinationals.[427] The chairman of the committee is reported to have said that Nigeria was on the verge of embracing the out-sourcing[428] initiative in order to earn foreign exchange from non-oil resource.[429]

What the chairman did not mention is that, in order for the out-sourcing dream to become a reality, several factors have to be in place.[430] The outsourcing of business

---

426 National Telecommunications Policy Chp 7.1 (iii).

427 Ezigbo 17th Oct 2005 *Thisday*.

428 Outsourcing is the management and/or day-to-day execution of an entire business function by a third party service provider. It is carried out by company A, contracting with another company B or person to do a particular function. According to the 2004 Economic Report of the President:

> One facet of increased services trade is the increased use of offshore outsourcing in which a company relocates labor-intensive service industry functions to another country. For example, a U.S. firm might use a call center in India to handle customer service related questions. The principal novelty of outsourcing services is the means by which foreign purchases are delivered. Whereas imported goods might arrive by ship, outsourced services are often delivered using telephone lines or the Internet. The basic economic forces behind the transactions are the same, however. When a good or service is produced more cheaply abroad, it makes more sense to import it than to make or provide it domestically.

See Council of Economic Advisers *Economic Report of the President* 229 [online]. See also Mankiw and Swagel *The Politics and Economics of Offshore Outsourcing* 7 [online].

429 See n 427.

430 According to Van Der Linden and Hengeveld, the core factors that must be present in a country seeking to attract outsourced work are:

- Knowledge

services offshore is now an established practice and the requirement for a transparent legal and regulatory regime is a top priority for the big companies and financial institutions that outsource some of their business processes offshore. The risks arising from non-compliance with privacy laws is a key factor in a company's assessment of whether to outsource services or not. Recurring reports in the media about breaches of data security and identity thefts around the world have focused attention on the need for stringent privacy protection measures.[431] The reports have triggered a backlash of legislative interventions to secure data protection particularly in the US.[432] Companies in the US and EU are now under increasing pressure from legislations that insist on them guaranteeing the privacy of their customers' financial and medical data.[433]

- Exposure to the international working culture
- Access to a high-quality infrastructure
- Awareness of cultural differences
- Mastery of English
- Investment into the local economy by large international companies
- Creation or expansion of a potential niche
- The political stability of a country
- Collaboration between the government, higher educational institutions and industry

See Van Der Linden and Hengeveld *Critical Success Factors for Obtaining Outsourcing Projects* 1-4 [online]. See also Pai and Basu *Offshore Outsourcing* [online].

431 See Privacy Rights Clearinghouse *Chronology of Data Breaches* [online]. The Privacy Rights Clearinghouse website contains links to other sources of information on data security breaches. Also, a widely publicised sale of customer IDs by an Indian call-centre staff in April of 2005 generated extensive discussions on the merits of outsourcing, prompting many enterprises to re-evaluate their assessments about the adequacy of data privacy and security laws in countries like India. See 23 June 2005 *Daily Mail* online.

432 In 2005 alone, several Bills were introduced in the American Senate and House of Representatives to mitigate identity theft, ensure privacy, provide notice of security breaches, require reasonable security policies and procedures to protect computerized data containing personal information and protect individual rights with respect to personally identifiable information. Other Bills introduced seek to establish procedures for the protection of consumers from misuse of, and unauthorized access to sensitive personal information contained in private information files maintained by commercial entities engaged in, or affecting, interstate commerce. The Bills are:

S 1789 Personal Data Privacy and Security Act, introduced 29/9/2005
HR 4127 IH Data Accountability and Trust Act (DATA), introduced 25/10/2005
S 500 Information Protection and Security Act, introduced 3/3/2005
HR1069 Notification of Risk to Personal Data Act, introduced 3/3/2005
S 1336 Consumer Identity Protection and Security Act introduced 29/6/2005
HR 3501 Consumer Access Rights Defense Act (CARD) introduced 28/7/2005
HR 3374 Consumer Notification and Financial Data Protection Act introduced 7/21/2005
HR 3997 Financial Data Protection Act of 2005 introduced 6/10/2005

See The Library of Congress (Thomas) *Bills, Resolutions* [online].

433 For example, the Federal Information Security Management Act (or Gramm-Leach-Bliley Act) of 1999 requires financial services companies in the US to create privacy policies that govern how information can

With the global outsourcing industry projected to continue its impressive growth, it is easy to see why the Nigerian government and the private sector are eager to participate in the global industry.[434] However, the requirement for a transparent legal and regulatory environment will pose a very serious obstacle to the realisation of this dream of capturing a good portion of the outsourcing market. This is because the risks arising from the handling of information touch three key areas of concern to the information economy:

- Privacy
- Intellectual property rights
- Infrastructure security

The protection of these core interests of ICT users (whether for personal or business purposes) should be of utmost concern to the government and regulatory authorities. The Nigerian regulatory regime has not adequately addressed these risks.[435] Two of the key objectives of the NTP are:

- To guarantee the privacy, integrity, accuracy, confidentiality, security, availability, and quality of personal information.
- To promote electronic trade, business and commerce.[436]

To achieve these objectives, as well as other similar objectives, the NITDA is expected to sponsor and promote the enactment of relevant IT laws that guarantee freedom of access to information and establish rights in respect of information. Furthermore, it should promote laws for the protection of online transactions, privacy and

---

be shared within and between institutions. Also, the Health Insurance Portability and Accountability Act of 1996 (or HIPAA), governs how US health-care institutions handle sensitive patient information.

434 A study by the Federal Deposit Insurance Corporation (FDIC) of the US in 2004 on outsourcing (also known as offshoring) in the financial services sector observed that:

> "In spite of different estimates of growth levels, most believe that offshoring will continue to increase for the foreseeable future……the Tower Group estimates that the share of offshored global financial services IT spending has steadily increased, from 50 percent in 1996 to 56 percent in 2003. While difficult to project with certainty, there are strong indications that offshoring will continue to grow into the future."

See FDIC *Offshore Outsourcing* [online].

435 See par 5.4 above.

436 *National Policy on Information Technology* chp 2.2 3.

intellectual property rights.[437] Specifically, the NITDA is expected to sponsor and promote the enactment of a Data Protection Act for "safeguarding privacy of National computerised records and electronic documents."[438] To date, the NITDA has not submitted any draft Bill for an Act to protect personal data to the National Assembly.

For its part, the strategic thrust of the NCC for the period 2004-2006, for example, was "Attaining Efficiency in the Telecoms Industry".[439] During this period, the emphasis of the Commission was on network expansion, technology advancement, convergence and management of competition. There was no corresponding emphasis on data protection and information security.[440] The Communications Act, 2003 does not have specific provisions that protect personal data. However, it requires the NCC to make interconnection regulations that address the protection of intellectual property rights and commercial information.[441] In 2003, the NCC published interconnection regulations under which it may impose conditions in interconnection agreements to ensure:

> The protection of data, to the extent necessary to ensure compliance with relevant legal and regulatory provisions on the protection of data, including protection of personal data, the confidentiality of information processed, transmitted or stored and the protection of privacy.[442]

The above provision notwithstanding, there is no law on the protection of data (including personal data), or on the confidentiality of information processed, transmitted or stored. Furthermore, the Consumer Affairs Bureau[443] established by the NCC to protect the consumer, has drawn up a weak Bill of Rights which makes no

---

437 Id at 33.

438 Id at 41.

439 Ndukwe *NCC Policy and Strategic Thrust - 2005 and Beyond* (2004) 6 [online].

440 Id at 13-15.

441 See s 99 Communications Act, 2003.

442 See n 423, Part IV Regulation 13.4 (b).

443 The Bureau was established in 2001 "to inform, educate and protect all the consumers of telecommunications services in Nigeria." See Consumer Affairs Bureau (Nigeria) webiste [online].

mention of data protection.[444] The availability of personal information profiles resulting from the use of information and communication technologies is of considerable interest not only to the individual to whom the information points, but also to law enforcement, national security, public safety organisations and the commercial sector.[445] Those nations, and indeed individuals who seek to participate in the global network economy, must agree to abide by the norms and rules that order activities in these globally networked economic and communication systems in order to minimise conflicts and maximise benefits. Information privacy and data protection have become frontline international trade issues thanks to the European Union's Directive on data protection.[446]

While most of the technologically advanced countries, and indeed some not so technologically advanced ones, have improved their laws on the transmission and protection of data, Nigeria is yet to enact such laws even in the face of clear policy expressions to do so. Any talk therefore about achieving the kind of success which India and lately South Africa have achieved in the area of call centre outsourcing, will remain a mere wishful thinking. Without enacting the appropriate data protection laws, it will be very difficult to persuade any sizeable corporation in Europe and the US to outsource the handling of its data to Nigerians.

It is therefore necessary to build trust in the telecommunication system by ensuring that a proper balance is maintained between, on the one hand, the need for personal information privacy and, on the other, the need for lawful access to information by law enforcement/state security agents and ordinary commercial interests. Building trust in the system requires the protection and enforcement of privacy rights of the people who use the system. What constitutes privacy, its origins, the threats to it and its relevance to the Information Society is examined in the next chapter.

---

444 Ibid.

445 Gow *Privacy and Ubiquitous Network Societies* 1 [online].

446 See Singleton *Privacy as a Trade Issue 2* [online]. The South African Law Reform Commission (SALRC) identifies international trade as a primary motivation in seeking the enactment of data protection laws that fit the EU standard. See South African Law Reform Commission (SALRC) *Privacy and Data Protection* (Discussion Paper 109) vi.

CHAPTER 4

THE LEGAL PROTECTION OF PRIVACY: A HISTORICAL, SOCIOLOGICAL AND PHILOSOPHICAL OVERVIEW

1. INTRODUCTION: THE RISE OF PRIVACY PROTECTION

This chapter will briefly explore the rise of privacy and present a historical, sociological and philosophical overview of the concept, contrasting the African and Western perspectives. It will examine the state of Nigeria's privacy law and whether it addresses the vulnerability of the individual's personal information to being misused or abused in the Information Age. The chapter will also examine the risks posed by the information and communication technologies to privacy generally and information privacy in particular. Nigeria's responses to the risks and the possible ways of safeguarding against them will also be examined.

The advent of the global communications networks has raised public awareness of the issues relating to privacy generally and in particular, information privacy.[447] This

447 For example, in June 2013, Edward Snowden, an IT specialist working for US contractor Booz Allen Hamilton, revealed in a video interview with Glenn Greenwald and Laura Poitras, aired on many news networks, that he was the source of the National Security Agency (NSA) files published that week in the *Guardian* and the *Washington Post* newspapers. Snowden said his motivation for revealing the large-scale electronic eavesdropping and interception of electronic data by the NSA and its British counterpart, GCHQ, was to launch a global debate on the limits of government surveillance and interception of personal information.

According to the *Guardian* (UK) newspaper, the Snowden files reveal a number of mass-surveillance programmes undertaken by the NSA and GCHQ. The agencies are said to be able to access information stored by major US technology companies, often without individual warrants, as well as mass-interception of data from the fibre-optic cables which make up the backbone of global phone and Internet networks. The newspaper reports that the spy agencies have also worked to undermine the security standards upon which the Internet, commerce and banking rely. The Snowden revelations have raised public awareness and concerns about growing domestic surveillance, the scale of global monitoring, the trustworthiness of the technology sector, whether the agencies can keep their information secure, and the quality of the laws and oversight keeping the agencies in check. In the case of the British agency, GCHQ, it is required to abide by the European Convention on Human Rights. See *The Guardian* "NSA Files" [online]. Furthermore, the *Guardian* also reported that the NSA collects almost 200 million text messages a day

is due mainly to the fact that information and communication technologies have increasingly facilitated the collection of diverse data from diverse sources at high speed and volume. The raw data can then be processed by these same technologies into usable information which can be linked to identifiable individuals.[448] This is one of the defining characteristics of the Information Society. In describing the Information Society and the role information plays in it, Sieghart[449] noted that:

> More transactions will tend to be recorded; the records will tend to be kept longer; information will tend to be given to more people; more data will tend to be transmitted over public communication channels; fewer people will know what is happening to the data; the data will tend to be more easily accessible; and data can be manipulated, combined, correlated, associated and analyzed to yield information which could not have been obtained without the use of computers.

The collected and processed information is now a commodity easily traded between small and big businesses and becomes valuable to the owner of the compiled information database. The Clinton administration acknowledged that:

> Information is one of the nation's most critical economic resources, for service industries as well as manufacturing, for economic as well as national security. By one estimate, two-thirds of U.S. workers are in information-related jobs, and the rest are in industries that rely heavily on information. In an era of global markets and global competition, the technologies to create, manipulate, manage and use information are of strategic importance for the United States. Those technologies will help U.S. businesses remain competitive and create challenging, high-paying jobs. They also will fuel economic growth which, in turn, will generate a

---

from across the globe, using them to extract data including location, contact networks and credit card details, according to top-secret documents provided by Edward Snowden. According to the Guardian, the untargeted collection of text messages from mobile phones across the world is made possible by an NSA programme codenamed Dishfire, which is able to collect "pretty much everything it can". The Guardian notes that the NSA "has made extensive use of its vast text message database to extract information on people's travel plans, contact books, financial transactions and more – including of individuals under no suspicion of illegal activity." See Ball 16th January 2014 Guardian (UK).

448 See n 408.

449 Sieghart *Privacy and Computers* 75-76.

steadily-increasing standard of living for all Americans.[450]

If information is one of the critical resources of the new economy and global competition, and the technologies that help to create, manipulate, manage and use information are of such strategic importance, the question that arises is why the synergy between these two resources has created such great concern in the minds of people who are the objects and subjects of these synergy.

The fact that relatively disparate bits of data are collected, processed and maintained in centralised computer data banks, and become aggregated into information that is identifiable to specific individuals, may be one reason for this concern. A more significant issue however, is that when "[a] computer operator with access to electronic information data banks can quickly and easily rearrange facts, incorporate new material, compile multiple databases and make other transformations of information."[451], the result is seen as a dangerous synergy. It is this particular function of the synergy that has given fuel to the vigorous campaigns worldwide for information privacy.

The development of the Internet along with the advent of e-commerce has further amplified the easy and ready access to both personal information and information in the public domain. This easy access has raised public policy issues concerning privacy. These issues, as Regan asserts, are often "defined in terms of an invasion of privacy."[452] The result is that for the Western developed societies, "The citizens … want privacy but feel it is extinct. They are aware of the loss of privacy, but feel powerless to defend themselves against intrusive practices."[453]

For the developing countries of Africa, the concept of privacy is not as well developed as in Europe and North America. Indeed, it has been suggested by Bakibinga,

---

450 IITF *National Information Infrastructure* [online].

451 Nimmer and Krauthaus 1992 *Law & Contemp Probs* 107-108.

452 Regan *Legislating Privacy: Technology, Social Values and Public Policy* 2.

453 Davies "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity" 147.

concerning Ugandans, that some of the citizens are "privacy myopic".[454] Nevertheless, one fact that holds true for both developed and developing countries in a globally connected world is that their societies are more or less caught in an underlying tension between the need to protect the privacy rights of individual citizens and the need to secure the community as a whole.

The individual's desire to protect his or her privacy often clashes with the community's need to obtain information that would enable the leaders to better manage its affairs. It becomes a fundamental issue to decide who may determine when, where, how and why information should be divulged, not the least because "[p]rivacy does not have a universal value that is the same across all contexts. The value of privacy in a particular context depends upon the social importance of the practice of which it is a part."[455] It is perhaps this singular quality, (i.e. not having a universal value that is the same across all contexts) that gives privacy such a contentious character.

1.1 What is Privacy?

1.1.1 The concept of privacy

For a concept that has become such an important theme in contemporary socio-political and legal concerns in the 21st century, privacy remains a challenging concept to define. Solove[456] describes privacy as a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. He describes the concept of privacy as a product of norms, activities, and legal protections and therefore culturally and historically contingent.[457] This cultural and historical

454 Bakibinga *Electronic Privacy in the Telecommunications Sub-sector* [online].

455 Solove 2002 *Cal L Rev* 1093.

456 Solove *Understanding Privacy* 1.

457 For example, norms about nudity, bathing and concealing bodily functions have varied throughout history and in different cultures. While it is widely accepted today that the naked body is private in the sense that it is generally concealed, that was far from the case in ancient Greece and Rome. According to Simon Goldhill, men exercised naked in the gymnasium in ancient Greece while men and women bathe together

contingency is evident today in the rich diversity of cultures across the world and the multiplicity of attitudes and approaches to privacy in different regions of the world. It accounts also, for the diversity of opinions on the meaning and essence of privacy. According to Robert Gellman, "[l]awyers, judges, philosophers, and scholars have attempted to define the scope and meaning of privacy, and it would be unfair to suggest that they have failed. It would be kinder to say that they have all produced different answers."[458]

Daniel Solove identified six broad headings under which the myriad of definitions of the concept of privacy may be discussed:

- the right to be let alone;
- limited access to the self;
- secrecy;
- control of personal information;
- personhood; and
- intimacy.

He acknowledges that although these headings often overlap, yet each has a distinctive perspective on privacy.[459]

The diverse perceptions of privacy evident in the many definitions of the concept can be distilled into two major views of the concept of privacy. The first view is made up of those definitions that present privacy as limited access to self; it explains privacy in terms of the extent to which we are known to others and the extent to which others have physical access to us. It emphasises seclusion, withdrawal, and avoidance of interaction with others. Ruth Gavison[460], a major proponent of this view, breaks

---

naked in ancient Rome. See Goldhill *Love, Sex, and Tragedy: How the Ancient World Shapes Our Lives* 15, 19.

458 Gellman "Does Privacy Law Work?" 193. Commenting on the multiplicity of privacy definitions, David Flaherty noted that "… philosophers continue to bemuse themselves with this important activity, it would appear, while individual authors parade their ingenuity with increasingly obscure, and obscuring, definitions." See Flaherty "Controlling Surveillance: Can Privacy Protection Be Made Effective" 167 at 171.

459 See n 455 at 1092.

460 Gavison 1980 (89) *Yale L J* 421.

down privacy into three basic components: secrecy, anonymity and solitude. According to her, "[s]ecrecy, anonymity, and solitude" are shorthand for "the extent to which an individual is known, the extent to which an individual is the subject of attention, and the extent to which others have physical access to an individual."[461] Another proponent of this view is Alan Westin,[462] who identified four states of privacy: solitude, intimacy, anonymity and reserve.[463]

The second group of definitions puts more emphasis on the control individuals have over information about their lives. Privacy is seen as control over information; it is not simply limiting what others know about you, but controlling the access to such information. An essential element in this view of privacy is individual autonomy by which the individual can control personal information in a meaningful way. Two eminent proponents of this view of the concept of privacy are Prof. C. Fried[464] and Arthur Miller.[465]

While it is commonplace to lament the great difficulty in reaching a satisfactory definition of the concept of privacy, there appears to be a consensus about the existence of a private and public sphere in every citizen's life. John Stuart Mill, writing about the private/public sphere of privacy, noted that:

> There is a circle around every individual human being, which no government, be it that of one, of a few, or by the many, ought to be permitted to overstep; there is a part of the life of every person who has come to years of discretion, within which the individuality of that person ought to reign uncontrolled either by any other individual or by the public collectively. That there is or ought to be some space in human existence thus entrenched around and sacred from authoritative intrusion, no one

461 Id at 433.

462 Westin *Privacy and Freedom* 31.

463 Ibid. In the state of solitude, the individual is separated from the group and freed from the observation of other persons. Intimacy refers to being alone with a small group (e.g. family), to the exclusion of others and concerns close relationships. Anonymity refers to being unrecognised in a public place; the individual, even while in public, still seeks and finds freedom from identification and surveillance. Reserve is based on the creation of a psychological barrier against unwanted intrusion; it is the desire to limit disclosures to others by holding back communication.

464 Fried 1968 (77) *Yale L J* 475.

465 Miller *The Assault on Privacy* 25

> who professed the smallest regard to human freedom or dignity will call into question.[466]

Although the line of distinction between the private and public sphere is oftentimes blurred and subject to much debate, it is inevitably in the context of the private and public spheres of human existence that claims to privacy arise.[467] The extensive scholarly, judicial and philosophical writings on privacy have produced a plethora of diverse definitions of privacy but no universally agreed definition.

1.1.2 Defining privacy

Although this thesis will focus on "information privacy", the inherent difficulty of defining with exactitude the concept of privacy remains. For Wacks, however, the many attempts to define privacy are inadequate in so far as they usually proceed from different standpoints and the attempted definitions themselves usually beg more questions than they answer.[468] His premise is that the meaning of privacy is already embedded in legal processes wherever the right to privacy is accorded. For example, the meanings attributed to privacy are those encapsulated in the vocabulary of the courts in determining whether the right lies or not, or in the case of statute, in the statutory definition of the right. In other words, meanings are attributed to privacy wherever it is being mobilised. As Foord pointed out, Wacks' theory of embedded definition assumes that the fundamental values attached to privacy are adequately expressed in the various statutes and causes of action and their case

---

466 Mills *Principles of Political Economy* 279; the concept of the public and private sphere is traceable to Aristotle's distinction between the public sphere of political activity (*polis*) and the private sphere associated with family and domestic life (*oikos*). See DeCew *Privacy* [online]. See also Gavison 1980 (89) *Yale LJ* 369.

467 It was in the context of a public/private dichotomy in the affairs of men, that Warren and Brandeis articulated their theory of a right to privacy. They envisaged a private sphere of personal matters that needed to be protected from the public. The right to privacy was to prevent the public from intruding on that which was private. What was private related solely to the individual, while what was public related to the community or society at large. See Warren and Brandeis 1890 (4) *HLR* 193. David Flaherty also makes the point that the North American colonists were concerned about keeping certain aspects of their lives private, away from the eyes, ears and minds of the rest of society. See Flaherty *Privacy in Colonial New England* 248.

468 Wacks *Law, Morality and the Private Domain* 214.

law.[469] The reality, however, is that the whole gamut of legal, sociological and philosophical discourse on the concept of privacy, clearly show that it is a deeply contested concept.

Cooley, in one of the earliest definitions of privacy, asserts that it is "the right to be left alone."[470] Cooley's simple definition is deemed by Gavison as inadequate because a great many instances of "not letting people alone" cannot readily be characterised as invasions of privacy. According to her, requiring people to pay their taxes, go into the army or punishing them for murder are just a few of the obvious examples.[471] Her definition of privacy is a reflection of her focus on access to the person.

Gavison's proposition that privacy is lost whenever other people obtain information about an individual, pay attention to such individual, or gain access to him or her, is not without a problem; just as it is not every instance of not letting people alone that results in breach of privacy as she rightly asserts, so also, it is not every instance of others having access to us or receiving information about us that results in a loss of privacy.[472] A man may indeed suffer loss of privacy and yet not be in a position to sue because he consented to the intrusion in the first place or perhaps some other ground justifying the intrusion exists.

Wacks suggests that for an intrusion upon an individual's solitude to be accorded privacy protection, such intrusion must impinge upon the individuals "private" acts. The information relating to the private act must be such that it "relate[s] to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict its collection, use, or

---

469 Foord *Defining Privacy* 4.

470 Cooley *A Treatise on the Law of Torts* 29.

471 See n 460 at 437.

472 Mason speaks of asymmetrical relationships such as priest/penitent, therapist/patient, doctor/patient, lawyer/client, in which personal information is disclosed willingly by one to the other as for example the patient to his doctor in the hope of having his life saved or disease cured or the quality of his life improved. This information is of course captured in the doctor's files or database permanently and will be shared with other staff of the hospital on a need-to-know basis in order to achieve the cure the patient needs. In such a scenario Mason argues, it is understood that this personal information will be used to achieve the personal goal of the patient which he deems at the time to be more important than his privacy. See Mason *Tapestry of Privacy* [online].

circulation."[473] Information of an intimate and sensitive nature, such as a person's sexual preference, would qualify as truly private and thus worthy of protection in this context.[474] In the same vein, Neethling defines privacy as "… an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself or herself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he or she evidences a will for privacy."[475] According to Neethling, Potgieter and Visser, there are two "levels" or aspects of privacy infringement. One is the factual infringement in which the act of privacy infringement has actually taken place; the second aspect is that such infringement should be unreasonable in order to be actionable.

However, one of the most contested definitions of privacy is that which situates privacy squarely in the domain of control over information. This definition signals our right or intention to determine what information about ourselves is circulated outside the closed community of those to whom we freely disclose information, particularly of the personal sort. According to Charles Fried,[476] "[p]rivacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves."

1.1.3 Information privacy

As the information age continues to unfold its technological innovations, the right to privacy has inevitably evolved to address that aspect of privacy generally called information privacy which deals with the collection, use, and dissemination of personal data in information and communication systems.

Westin defines privacy as the "claim by individuals, groups or institutions to

---

473 Wacks *Personal Information: Privacy and the Law* 26.

474 It is not only sensitive personal information of a sexual nature that can qualify for protection; this is merely one example of the genre of "private acts" that, according to Wacks, should qualify for protection. The nature of the personal information in issue would often determine whether it is private or not. Apart from sexual behaviour, many would readily agree that information about a person's health, financial standing and confession to a priest, fall within the ambit of "private information or acts".

475 Neethling, Potgieter and Visser *Neethling's Law of Personality* 32.

476 Fried "Privacy" 209.

determine for themselves when, how and to what extent information about them is communicated to others."[477] This definition captures the essence of "information privacy" which is the focus of this thesis. It shall form the premise upon which the analysis of the policy issues created by or relating to the emergence of information technologies in the socio-legal landscape of Nigeria will proceed. In accord with Kang,[478] the focus of this thesis is on information privacy, because it is that sphere of privacy that is most readily affected in the cyberspace environment of an information-based economy in the Information Revolution era.

Cyberspace is a construct of diverse information and communication technologies within which the collection of personal information by governments and private bodies into databases has grown to such unprecedented level that it has made information privacy the linchpin of privacy advocacy in the 21st century. Information privacy advocacy led to the formulation of principles known as "fair information practices"[479]; these principles govern the collection and handling of personal information and were developed and adopted by national governments and international bodies such as the US Department of Health, Education and Welfare in 1973; the Organisation for Economic Co-operation and Development (OECD) in 1980 and the Canadian Standards Association in 1996.

National constitutions in many countries also recognise the control of personal information as a privacy right. For example, the Nigerian Constitution provides that "[t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."[480]

---

477 See n 462 at 31-32.

478 Kang 1998 (50) *Stan L Rev* 1205.

479 Fair Information Practices (FIPs) are a set of internationally recognized practices for addressing the privacy of information about individuals. For a brief history of FIPs, see Gellman *Fair Information Practices* [online].

480 S 37 Constitution of the Federal Republic of Nigeria, 1999.

1.2 The rise of privacy as a legal right

As a specific value and right, privacy did not come into focus until the 19th century. Indeed, it is said that "[t]he law of privacy is a 19th century American development. Before 1890, no American court had recognized a right of privacy."[481] In 1890, Samuel Warren and Louis Brandeis jointly wrote a law article in the Harvard Law Review that articulated the "Right to Privacy".[482] It emphasised the separation between the individual and the rest of the society. This right, which they defined as the "right to be let alone", echoes the Lockeian libertarian concern with the individual's rights and the securing of the boundary between him and the rest of the society. The "Right to Privacy" effectively set in motion the international discourse on privacy particularly in the United States of America.[483]

The Warren and Brandeis' article was written in reaction to what the authors perceived to be the menace of intrusive technology; advances in printing and photography technology in 1890 had reached a level which made it possible for practitioners of journalism to intrude upon the private premises of members of the public. Their article was written to protest the growing excesses of the press and the intrusive capabilities of their new technologies which made the public dissemination of details relating to a person's private life possible. They said:

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." ... The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury...[484]

---

481 Creech *Electronic Media Law and Regulation* 242.

482 Warren and Brandeis 1890 (4) *Harv L Rev* 193.

483 Solove 2002 *Cal L Rev* 1100.

484 See n 481 at 195-196.

Warren and Brandeis presented the right to privacy as an already existing common law right which embodied protections for each individual's inviolate personality. According to them, "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others ..."[485] To Warren and Brandeis, the right to privacy meant that each individual had the right to choose to share or not to share with others information about his or her "private life, habits, acts, and relations."[486] They contended that it was necessary for the legal system to recognize the right to privacy because, when information about an individual's private life is made available to others, it tends to influence and even to injure the very core of an individual's personality - "his estimate of himself."[487]

According to Dorothy Glancy,[488] Warren and Brandeis invented a legal theory which brought into focus a "right to privacy" by means of an ingenious evocation of a broad historical sweep in which such legal recognition and enforcement, derived from diverse areas of the law such as contracts, property, trusts, copyright, protection of trade secrets, and torts, appear as a natural and inevitable development.

The right to be let alone, which Warren and Brandeis articulated in their article, set the agenda for not only a more detailed analysis of the new concept of privacy, but also the efforts to define it. The profound effect that the article and Brandeis' later dissenting opinion in the American case of *Olmstead v. United States*[489] have had on American jurisprudence can be seen in a long line of cases.[490] For example, the American Supreme Court which had earlier held in the *Olmstead* case above, that wiretapping was not a violation of the Fourth Amendment of the constitution,

---

485 See n 481 at 198.

486 See n 481 at 216.

487 See n 481 at 197.

488 Glancy 1979 (21) *Ariz L Rev* 3.

489 277 US 438 (1928).

490 Some of the cases are: *Oklahoma Press Pub. Co. v Walling* 327 US 186, 204, (1946) where the Supreme Court cited Brandeis' dissent in the *Olmstead* case as making "the case for protected privacy". See also *Doe v Bolton* 410 US 179 (1973), *Eisenstadt v Baird* 405 US 438 (1972).

reversed itself in the latter case of *Katz v. United States*.[491] In many countries across the world, constitutional and statutory protections of privacy are very common today, thanks to Warren and Brandeis' articulation of the right to legal protection of privacy in 1890.

2. HISTORICAL, SOCIOLOGICAL AND PHILOSOPHICAL ROOTS OF PRIVACY

2.1 Introduction

In reviewing the historical, philosophical and sociological roots of privacy, it is pertinent to bear in mind that different peoples have different ideas about privacy and "[i]t is commonplace that privacy is culture specific: the matters which a particular society regards as 'private' can vary widely."[492] The intention here is neither to give an exhaustive discussion or review of the arguments for or against privacy nor to discuss the literature on the roots of the privacy discourse. It is rather intended to highlight the major differences and nuances in the perceptions of privacy in Western and African cultures and how these have shaped, and may likely shape the discourse and responses to privacy invasions. Particular reference will be made to the position in Africa/Nigeria.

2.2 Western intellectual and cultural traditions

The Western philosophical basis of privacy assumes there is a society that is made up of relatively autonomous individuals who need a measure of privacy in order to make rational self-determining decisions. This view of society traces its roots in the 17th century liberal political philosophy of John Locke which rests on the notion of the individual as the dynamic force behind social progress.[493] He believed that by nature, people are free and equal, having certain rights such as liberty, life and ownership of

---

491 389 US 347 (1967). The Supreme Court referred to the "right to be let alone" from Warren and Brandeis' 1890 article.

492 Michael *Privacy and Human Rights* 2.

493 Locke *The Second Treatise of Government* chp 2-7.

property and it was the task of the state to protect these rights.[494] It is this notion that gave birth to the liberal democratic traditions of Western societies which established a set of individual rights and duties in society. According to Bennett,[495] this notion assumes that an individual endowed with liberty, autonomy, rationality and privacy knows what his best interests are and should be allowed a private sphere untouched by others. It casts "the debate about privacy as a debate about boundaries: the boundary between the individual and the state, the community or some other collective concept."[496]

Locke's liberal concept of individualism is echoed in J. S. Mill's assertion that "[t]here is a circle around every individual human being, which no government, be it that of one, of a few, or by the many, ought to be permitted to overstep".[497] This idea of boundaries is premised on the primacy of individual rights which are guaranteed by means of a social contract whereby the people in a state conditionally transfer some of their rights in exchange for the protection of other rights such as life, liberty and property.

Thomas Hobbes[498] articulated the social contract theory in his book *Leviathan*[499] and concluded that men ought to submit to the authority of an absolute sovereign power. Although Locke and Hobbes expounded the social contract concept, their articulations of the concept were divergent. Under Hobbes' social contract theory, rational, free, and equal persons living in the "solitary, poore, nasty, brutish, and short state of nature"[500], agree to submit to some mutually recognised public authority in return for the protection of the public authority.[501] Hobbes tried to reconcile the idea of authoritarian monarchy with the then growing idea that

494 Ibid. See also Tuckness "Locke's Political Philosophy" [online].

495 Bennett *Privacy in the Political System* 8-9 [online].

496 Ibid.

497 Mills *Principles of Political Economy* 547.

498 Hobbes *Leviathan*.

499 Published in 1651.

500 Lloyd and Sreedhar "Hobbes's Moral and Political Philosophy" [online].

501 Ibid.

ultimate power was derived from people. His theory sought to show that the people had by their own will and action surrendered all their natural rights to the sovereign for the sake of self-preservation in order to escape the life of insecurity in the state of nature.[502] Craving a life of security and instructed by reason, they agreed to surrender their rights to a person or body of persons who become the sovereign thereafter. According to Hobbes, the surrender is total with no residual rights remaining in the people including the right to privacy.

Hobbes' presentation of the social contract theory agrees more with the ancient Greek political philosophy which posited that an individual can find true fulfilment, happiness and humanity only by renouncing his privacy and becoming a full citizen who shares every aspect of his life with other citizens.[503] This argument is buttressed by Bennett who suggests that Greek and Roman civilisations and the Renaissance period in Italy may have flourished on account of the lack of privacy.[504] Aristotle defined man as "*zoon politikon*" (political animal) having citizenship in a *polis*.[505] Citizenship meant full membership in the *polis*; the very notion of citizenship required full participation in the public sphere of politics (*polis*), hence his distinction between the public sphere of politics (*polis*) and the private sphere of family life (*oikos*). To function effectively in the *polis* as a citizen, one had to forgo his private sphere (privacy) and conduct the affairs of the community in public (*polis*) as a full member of the *polis*.[506]

According to Locke however, man in the state of nature did not live in a state of war or in constant fear but was in a state in which men were equal and free to act as they

---

502 Ibid.

503 This idea of the state's primacy also found expression in the derivative philosophy of ancient Roman thinkers such as Cicero, for as Cook says, "Rome conquered Greece and received Greek philosophy as a reward. It kept alive certain Greek ideas and transferred them to the western world in general." See Cook *History of Political Philosophy from Plato to Burke* 133. However, De Boni and Prigmore assert that privacy was an incomplete and imperfect concept in Rome; consequently the state took precedence over the individual whose noble duty it was to seek the common good. See De Boni and Prigmore *Privacy and the Information Economy* 537 [online].

504 Bennett *Regulating Privacy* 32.

505 The *polis* is the city-state.

506 See n 503 DeBoni and Prigmore.

thought fit within the bounds of the law of nature:

> The State of Nature has a Law of Nature to govern it, which obliges every one: And Reason, which is that Law, teaches all Mankind … that being all equal and independent, no one ought to harm another in his Life, Health, Liberty or Possessions.[507]

A fundamental difference in Locke's conception of the social contract was that there was no surrender of the natural rights enjoyed in the state of nature. Only the rights of interpreting and enforcing the law of nature (which all men had in the state of nature) were surrendered in order to protect their existing rights in a more effective manner.[508]

The consequence of Locke's social contract arrangement is the primacy of individual rights in which the individual no longer finds his fulfilment in being a member of a society, but the society derives its purpose and existence from its ability to guarantee the rights of the individual.[509] This liberal conception of the individual's primacy derives from the view of a person as "an isolated, autonomous individual … with inherent rights in the domain of the civil and the political"[510]

Locke's idea of the primacy of the individual and his rights runs counter to the earlier Greek/Roman political philosophy which espoused the primacy of the state. The libertarian foundations upon which the claims for individual privacy in Western cultures rests, is dependent upon the distinction between the individual and the state, in essence between the private and the public sphere.[511] Unlike the communal character of African culture which shall be discussed shortly, the liberal traditions of Western culture de-emphasise the inter-dependence of individuals in a community. The individual is autonomous, with a private identity which requires some boundaries to maintain his individuality. It is privacy therefore, that reinforces the

---

507 Locke *The Second Treatise of Government* sec 6 line 6-10.

508 Ibid.

509 See n 503 De Boni and Prigmore.

510 Pollis "Liberal, Socialist, and Third World Perspectives of Human Rights" 7.

511 See n 466.

boundary/barrier between the individual and the state.[512] Furthermore, it is said that the emphasis on individualism and property rights, which is prevalent in Western culture is at the root of Western perspectives on human rights.[513]

2.3 African/Nigerian intellectual and cultural traditions

The philosophical underpinnings of the concept of privacy enunciated above differ greatly from what obtains generally in Africa. Communalism plays a far greater role in the African context, in shaping attitudes than the 'rugged individualism' of Western culture. African traditional societies place a greater premium on social cohesion than individuality. Kigongo defines social cohesion as "a state of affairs whereby individuals in the society consistently pursue certain fundamental virtues on the basis of enhancing a common or social good"[514]

Traditional African social and political life is not only communal, but also subsumed under a hierarchical structure. According to Mbiti,[515] the African community uses a metaphysical and social hierarchy in a descending order beginning from God, to dead founders of clans or ethnic groups, to dead grand forefathers, to the living-dead, the elders, and then, to men, women, children, animals, plants and finally to inanimate beings. An elder takes precedence over youths, man over woman, and God over everyone and everything. Implicit in this hierarchy however, is social inequality, for men enjoy more rights than women.

Kigongo observes that, notwithstanding the communal nature of traditional African society, there is an underlying individuality which is inherently human in nature and survives any form of external influence. The potential for conflict between the common good of the community and the personal goals or ambitions is always present but coercively kept in check by the authority of the elders. He further argues that the colonial system facilitated usurpation of the authority and power of the

512 See n 466.

513 Leary *The Effect of Western Perspectives on International Human Rights* 17.

514 Kigongo *Concepts of Individuality and Social Cohesion* [online].

515 Mbiti *African Religions and Philosophy* 208.

elders by the contemporary political leaders who emerged through the manipulation of the colonialists and the dynamics of education, as the new social and political elite. The result is that in the post-independence states of Africa, these new leadership elite have established 'democratic' institutions in which the conflict between the individual and the 'elders' (the state) is now a social and political crisis expressing itself in agitations for more freedoms or rights.[516]

Africans regard culture as essential to their lives and well-being; culture in the context of African philosophy, is said to be an "open-ended resource of social meanings upon which members of a community draw to mediate the contingencies of their everyday lives."[517] According to Coetzee,[518] culture indicates the resources of a community's material and moral worlds; it is through these that a certain group of people delimits itself as a community. A community is therefore, an ongoing association of men and women who have a special commitment to one another and a distinct sense of their common life. A communal or social identity is the community's characteristic way of life, developed over a considerable period of time.[519]

Individualism, the hallmark of Western culture, is said to pertain to societies in which ties between individuals are loose; everyone is expected to look after himself or herself and his or her immediate family.[520] Individualism thus engenders the seeking of one's own rights and freedom. Communalism on the other hand, is a social order in which the supremacy of the community is culturally and socially entrenched, and society is hierarchically structured.[521] Moemeka argues that experts on Western culture wrongly identify the core characteristics of communalism as collectivism; this error, he asserts, is responsible for the erroneous identification of Nigeria as a collectivist society when in fact it is fundamentally communal.[522] He goes on to assert

---

516 Ibid.

517 Coetzee "Particularity in Morality and its Relation to Community" 317.

518 Ibid.

519 Ibid.

520 Hofstede *Cultures and Organisations: International Cooperation and its Importance for Survival* 50.

521 Moemeka 1998 (48) *Journal of Communications*124.

522 Id at 120.

that communalism is the fundamental culture of most developing societies, particularly in Africa.[523]

2.4 Libertarianism versus communalism

The libertarian tradition, exemplified by individualism, is distinguishable from the communal tradition by the fact that a person is "an isolated, autonomous individual … with inherent rights in the domain of the civil and political."[524] The communalist tradition, of which Africa is a principal example, on the other hand, regards the individual and self to be almost totally dependent on, and subordinate to the community. According to Mbiti, the individual does not have much scope for self-determination outside the African family and community.[525] He asserts that:

> Whatever happens to the individual happens to the whole group, and whatever happens to the whole group happens to the individual. The individual can only say: "I am, because we are, and since we are, therefore I am."[526]

The basic difference between the African communal perspective and the Western libertarian perspective is that under the Western tradition, an individual can claim a right, even against the society at large.[527] On the other hand, proponents of the communal perspective argue that human rights are irrelevant since they devolve on individuals, whereas the communal societies of Africa value their families and communities more than they emphasis individualism and rights.[528] Western-style

---

523 Id at 125. In support of this assertion, see Coetzee (fn 517 above), Markus and Kitayama 1991 (98) *Psychological Review* 224. Note however, Gyekye's observation (while conceding that communalism is a generalised feature of African communities), that the individual, though undeniably bound to his family and community, possesses a distinct personhood and volition of action. This combined personhood and community membership enables the individual to take personally enhancing and socially responsible decisions and actions. See Gyekye K *The Unexamined Life: Philosophy and the African Experience* (1988) 31-32.

524 See n 510 at 7, 5.

525 See n 515.

526 See n 515 at 109. See however Elias *The Nature of African Customary Law* 94 where he asserts that "… the truth is that the African individual is neither a robot nor a peacock. He is, like any other human species, a social animal."

527 Howard "Group versus Individual Identity in the African Debate on Human Rights" 178.

528 Id at 162.

privacy is seen as promoting a contrary ethos of individualism;[529] consequently, collective decisions, community consensus, loyalties to one's group and respect for leaders are the core values stressed in a typical African society.[530]

2.5 Privacy in African/Nigerian communal cultures

In reviewing the extensive literature on communalism and cultural relativism in Africa and their effect on the human rights discourse, one striking observation is the fact that privacy, as a normative value, does not feature prominently in the discourse. This suggests that privacy, to the extent that it seeks to set boundaries between the individual and other members of the community at large,[531] is at odds with the strong communal ethic of African societies. It is a right enjoyed by an individual and therefore capable of creating tensions between the individual and the community. The typical African community is characterised by openness and interdependence. For example, the responsibility for socialisation of a new child born into the family and community is shared between the child's parents, grandparents (if alive), the extended family and neighbours.[532]

Gbadegesin observes that the process begins in the family apartment, the household compound and then the larger community.[533] Privacy in the African context, whether locational or informational, is hampered by the fact that the individual is socialised to expect a good measure of openness in his or her dealings with other members of the extended family, and the community at large. For example, in a typical Yoruba

529 Umozurike 1988 (1) *Afr J Intl L* 65.

530 Paul "Participatory Approaches to Human Rights in Sub-Saharan Africa" 233.

531 The Western debate about privacy is seen essentially as seeking to set up boundaries; the boundary between the state and individuals and between individuals *inter se*. For fuller discussions about the debate that has been going on in the last three decades on international human rights, Western intellectual ethnocentrism and the relativist perspective by some writers that suggest there is an "African" concept of human rights, see Welch E C and Meltzer R I (eds) *Human Rights and Development in Africa* (1984); Pollis A and Schwab P (eds) *Towards a Human Rights Framework* (1982); Donnelly J and Howard R E *International Handbook of Human Rights* (1987); Howard R E *Human Rights in Commonwealth Africa* (1986); Mojekwu C "International Human Rights: The African Perspective" in Nelson J L and Green V (eds) *International Human Rights: Contemporary Issues* (1980) 85-95; Howard and Donnelly 1986 (80) *Am Polit Sci Rev* 801-817.

532 Gbadegesin *Individuality, Community and the Moral Order* 292.

533 Ibid.

family of south-western Nigeria,

> ... everyone eats and drinks and talks in the full view of everybody else; ... quarrels and rebukes take place within the full hearing of neighbours ... each individuals weaknesses and vices are open to the observation of other[s] ... This makes exclusive family life in the Western sense impossible. Only a limited amount of privacy is possible.[534]

It is thus easy to see why, in an environment where openness is the default mode of interaction, the desire to enforce one's personal privacy can be easily interpreted as a desire for "secrecy". The other members of the community could readily see such an individual as seeking to "hide something". This thinking is discernible in the arguments of the proponents of freedom of information in Nigeria. They argue that privacy is tantamount to secrecy, behind which corruption and maladministration flourish. Privacy of course does more than hide shameful conduct or corrupt practices and should not be seen merely as something sought by criminals or deviants.

The openness that characterises the African cultural milieu would undoubtedly be a hindrance to privacy in the Western normative sense. This openness calls to question whether a Western style agitation for privacy can gain the type of robustness in Africa that privacy advocacy in the West is known for. In so far as the Western concept and enforcement of privacy is focused on the individual, by providing him/her a private space,[535] and the right or capacity to control, or at any rate monitor the flow of information about himself/herself,[536] the ethic of communalism will present resistance to the wholesale adoption of a privacy concept that focuses on the individual.

While the communal ethic of African societies is generally accepted, it is necessary to

---

534 Fadipe *The Sociology of the Yoruba* 101-102. However, this quote from a column in a Nigerian newspaper, Lagos Weekend, points to a trend towards seclusion and therefore a greater appreciation of privacy: "[o]nce in the city of Lagos, this virtue [of openness and being one's brother's keeper] is no longer to be found. This is because there has been a cold craze … branded "fenceophobia" … and its symptoms include a tendency for seclusion. Many people are getting secluded in Lagos and one cannot even know his neighbours again. This is all part of being Westernised." See Olusanya 1970 (32) *J Marriage & Fam* 150-155.

535 See n 495 where Bennett characterises liberal notions of privacy as seeking to lay boundaries between the individual and the state, the community or some other collective concept.

536 Eg, the "right to informational self-determination" exemplified in the EU *Data Protection Directive* (95/46/EC). See also the German case of 65 BVerfGE (Decisions of the Federal Constitutional Court) 1 42 (1983).

note also, as Howard has pointed out, that although the ethic of communalism still has a strong hold on many African societies, the practice is changing. This is due to economic crises, urban under and unemployment and highly lopsided social stratification.[537] It has become increasingly obvious to the average African that, in his country's pursuit of economic development, urbanisation has become a desirable component of national development to ensure a reasonably contented existence. With urbanisation, there is also a growing crisis concerning his traditional values and the creation of new ones. As many African societies pass from traditional to modern society and from rural to urban life with their complicated money economy and international trade, his traditional values are bound to come in conflict with the demands of modern technological lifestyles.

3. RIGHT TO PRIVACY IN NIGERIA

3.1 Introduction

In Nigeria, diverse ethnic groups were merged together by the British colonial authorities to form the new state. In the absence of a strong, viable and relatively autonomous private sector, state power has over the years been seen as the best means of social distribution of national wealth. Consequently, the need to have rights which ensure that state power as exercised by governments will not be used to perpetuate sectional interests became necessary. The inequalities among the constituent groups in terms of size, resource endowment, socio-economic development, access to state power and the struggles to redress them make the control of government institutions of paramount concern to the different groups. Therefore, to guarantee and safeguard rights, correct historical imbalances and inequalities between and among various groups in a plural and divided society like Nigeria, fundamental human rights have been entrenched in virtually all the constitutions of Nigeria since independence.

On attainment of independence in 1960, Nigeria, like many of the other African countries of the period, sought acceptance and legitimacy in the international comity of nations through membership in the United Nations. To demonstrate their

[537] See n 527 at 165.

preparedness to operate within the parameters of the norms of international law and relations, these countries affirmed and adopted the ideals of the UN, its charter and covenants. One of such ideals was the Universal Declaration of Human Rights (UDHR). This is why all the Nigerian constitutions from 1960 to 1999 have reflected the ideals articulated in the UDHR and other covenants of the UN, including the right to privacy.[538]

The *African Charter on Human and Peoples' Rights* on the other hand, does not make provision for the protection of privacy in any of its articles.[539] There is however provision for privacy in the *African Charter on the Rights and Welfare of the Child*.[540] The fact that privacy is not mentioned at all in the main charter suggests that at the time of its formulation, privacy was not seen as a right necessary for Africans to achieve self-actualisation. This is all the more persuasive considering that the African charter was formulated and adopted 33 years and 15 years respectively, after the UDHR and the ICCPR had been in operation. It is therefore arguable that by 1990 when the Charter on the Rights of the Child was adopted, the idea of privacy as an essential right had become recognised and accepted.

Of all the key mechanisms adopted worldwide to safeguard the rights of the citizens and inhabitants, the constitution is perhaps the most fundamental safeguard of the rights of a country's citizens and residents. Constitutions normally stipulate the scope of the fundamental human rights of the citizens, and in some cases, spell out the circumstances under which derogation from those rights may be allowed. Nigeria has experimented with 6 Constitutions from independence in 1960 to 1999.[541] All of them have unfailingly guaranteed the protection of human rights and made these rights enforceable, so that citizens whose civil or political rights are infringed upon

---

538 A 12 *Universal Declaration of Human Rights* (1948). It is also protected in a 17 of the *International Covenant on Civil and Political Rights* (1966), a 16 of the United Nations *Convention on the Rights of the Child* (1989), and a 14 of the United Nations *Convention on Migrant Workers* (1990).

539 The *African Charter on Human and Peoples' Rights* (OAUDoc. CAB/LEG/67/3 rev.5; 1982 (21) ILM 58).

540 African *Charter on the Rights and Welfare of the Child* (1990). It is indeed strange that privacy rights are granted to children and not their parents.

541 The Constitutions are: Constitution of the Federation of Nigeria, 1960; Constitution of the Federal Republic of Nigeria, 1963; Constitution of the Federal Republic of Nigeria, 1979, Constitution of the Federal Republic of Nigeria, 1989, Constitution of the Federal Republic of Nigeria, 1993 and Constitution of the Federal Republic of Nigeria, 1999.

either by the state or another individual can institute legal actions against such individual or the state for redress.[542]

3.2 Statutory protection of privacy

3.2.1 Introduction

There are statutory provisions that regulate activities in various sectors of the economy; some of these provisions concern the use of personal information. Although there is no general and comprehensive data protection law in operation now, there are however efforts being made to correct the situation. These efforts will be evaluated in chapter 7. The few available laws that deal with the protection of private data are fragmented, both with regard to their subject matter and to their administration. The protections provided by the said statutes are often ancillary to the main objects of the statutes.[543] For example, the Wireless Telegraphy Act[544] is primarily concerned with the regulation of wireless telegraphy, but because personal data passes through the apparatus of the wireless telegraphy, certain restrictions were enacted for the protection of such personal data.[545]

3.2.2 The relevant statutes

3.2.2.1 The Wireless Telegraphy Act

At a minimum level, the Act makes provisions for certain breaches relating to the protection of privacy and personal data in that it prohibits the interception and disclosure of personal messages. The Act makes it an offence for an employee to

---

542 Under s 46(3), the Chief Justice of Nigeria is empowered to make rules with respect to the practice and procedure of a High court for the enforcement of the fundamental rights contained in chapter 4 of the constitution. Consequently, the Fundamental Rights (Enforcement Procedure) Rules, Cap 62, Laws of the Federation of Nigeria, 1990 govern the procedure for enforcement of fundamental rights in Nigerian courts.

543 Eg the Corrupt Practices and Other Related Offences Act, 2000 is primarily concerned with investigation and prosecution of corrupt practices as defined in the Act; in the course of investigation of allegation of corruption, it is likely the Commission set up under the Act would come in contact with private data. S 43(1) & (2) of the Act requires the Commission to obtain a court order before an officer of the Commission can inspect and take copies of banker's books, accounts or any document belonging to or in the custody of the bank.

544 Vol 16 Laws of the Federation of Nigeria 2004.

545 Id s 10(1) (a) (b) & (c).

intercept personal data without authorisation, in the course of using any telecommunications equipment or facilities, with the intention of obtaining information relating to the content, sender or addressee of any message.[546] There is a proviso, however, that where such information is required in the course of a judicial proceeding or for the purpose of making a report, there shall be no liability.[547] Unfortunately, this proviso does not state the type of report and the purpose for which it should be required in order to justify the release of personal information without the consent of the subject of that information. The absence in the statute, of strict and clear parameters for the release of personal information goes contrary to the trend in other jurisdictions[548] where stricter measures are spelt out for the safety and integrity of personal data.

The Act also prohibits the provision of misleading information;[549] a person who "by means of wireless telegraphy" sends, or attempts to send any message which to his knowledge is false or misleading or is likely to prejudice the efficiency of any service or endanger the safety of any person commits an offence.[550] In real terms, the provisions are inadequate to the extent that they address only the conduct of an employee or an officer of a network service provider. The Act fails to provide protection against third party users who are not employed by the service providers. Because the Act criminalises these acts, an individual that is adversely affected thereby, has no opportunity to take up an action against the party responsible for the breach of privacy.

---

546 Id s 10(1)(a).

547 Id s 10(1)(c).

548 See n 479 above. See also OECD *Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data* (1980). Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981) and *Directive 95/46/EC of the European Parliament and of the Council of 1995*.

549 S 10(1)(a).

550 Ibid.

3.2.2.2 Telecommunications and Postal Offences Act[551]

Similarly, the Telecommunications and Postal Offences Act[552] prohibits the unauthorized communication to a third party of "any information relating to the movement of a mail bag or other postal matter or electronic mail".[553] In terms of addressing service providers' liability for personal data and privacy infringement, a measure of safeguarding has been put in place, but it is questionable whether these provisions on the protection of privacy and personal data in an electronic medium will meet the stringent rules of the EU on the trans-border flow of personal data.[554]

3.2.2.3 Statistics Act[555]

This Act makes provision for the collection of statistics in the federation. Under section 6 thereof, the statistician may by notice in writing demand "periodical or other information, estimates or returns" from the person or persons to whom the notice is addressed.[556] The statistician may also obtain information by interviewing any person or requiring that person to complete a form. Information obtained in this manner may be of a personal nature. The Act imposes a duty on any person required to furnish information to do so; the constitutionality of the Act in relation to the right to privacy has so far not been questioned.[557] The Act does, however, protect the data provided under section 6 by restricting the disclosure of such data under section 8. The information obtained may only be "published, admitted in evidence or shown to any person not employed in the execution of a duty under this Act"[558] with the written consent of the person making the return.

---

551 Vol 14 Laws of the Federation of Nigeria 2004.

552 Ss 18 & 25.

553 S 18.

554 See a 25 *Directive 95/46/EC*.

555 Statistics Act Vol 14 Laws of the Federation of Nigeria 2004.

556 S 6.

557 See however, the South African case of *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC) 1145, where a medical practitioner who was required under the South African Statistics Act to furnish census particulars and other information required of medical practitioners, complained that such requirement violated his right to privacy. The Constitutional court held that the mandatory provisions of the Act did not interfere with his right to privacy.

558 S 8(c).

3.2.2.4 NIPOST Act[559]

It is an offence under this Act for a mail delivery worker to unlawfully open or allow to be opened any postal article entrusted to him.[560] Similarly, the master of a vessel who unlawfully opens mail or other postal article entrusted to him commits an offence.[561]

3.2.2.5 Evidence Act[562]

Under the Evidence Act, the husband or wife of a marriage concluded under the Marriage Act,[563] cannot be compelled to disclose any communication made to him or her during the marriage, by any person to whom he or she has been married.[564] This protection of privileged information also applies to lawyer-client relationships. No legal practitioner is permitted to disclose any communication made to him in the course and for the purpose of his employment as such legal practitioner without the consent of his client.[565] He is also not permitted to state the contents of any document with which he has become acquainted in the course of and for the purpose of such employment. Also, no person can be compelled to disclose to the court any communication between him and his lawyer unless he offers on his own volition to be a witness, in which case he may be compelled to disclose such communication as a witness.[566]

---

559 Nigeria Postal Service Act.

560 S 29.

561 S 28.

562 Cap112 Laws of the Federation of Nigeria 1990.

563 Cap 218 Laws of the Federation of Nigeria 1990.

564 See s 161(3).

565 See s 170(1).

566 Nwadialo *Modern Nigerian Law of Evidence* 45. See also s 36(4)(a) of the 1999 Constitution which grants the courts discretion to exclude:

> … from proceedings persons other than the parties thereto, or their legal practitioners in the interest of defence, public safety, public order, public morality, the welfare of persons who have not attained the age of 18 years, the protection of private lives of the parties or to such extent as it may consider necessary by reason of special circumstances in which publicity would be contrary to the interest of justice.

3.3 The Common Law connection

Given the fact of Nigeria's colonial common law heritage, it is surprising that the development of the right to privacy in Nigeria has not followed the path in the UK. Nigeria's jurisprudence has benefited greatly from developments in English law. Decisions of English courts continue to enjoy strong persuasive authority in Nigerian courts. Until very recently, the English common law did not recognise the right to privacy. Notwithstanding this lacuna in the common law prior to 1998, a person who claimed that his right to privacy had been breached could nevertheless bring action against the defendant under the common law action for breach of confidence, trespass or defamation.[567]

In Nigeria, while the common law torts of trespass and defamation have been developed, the common law action for breach of confidence in defence of privacy rights has not followed the developments in England. The result is that the common law position on privacy in Nigeria largely remains what was the position in England prior to 1998. The fact that all of the Constitutions that Nigeria has had since independence have guaranteed the right to privacy, should have provided the courts with a platform from which to direct the development of the law of privacy. To understand the lack of development of common law-based privacy protection in Nigeria, it is necessary to take a look first at the development of what is now recognised as English common law of privacy.

3.4 Development of English common law protection of privacy

Prior to 1998, when the United Kingdom Human Rights Act was enacted, there was no right to privacy recognised by the common law. The House of Lords affirmed that no general tort of privacy existed in English law in *Wainright v Home Office*.[568] The Human Rights Act incorporated the *European Convention for the Protection of*

[567] The equitable remedy of confidentiality, torts linked to intentional infliction of harm to the person as well as administrative law principles relating to proper exercise of police powers, have been used by the courts to deal with cases in which a claim to privacy was made. See *Av B Plc* (2003) Q. B. 195, *Home Office v Wainright* (2001) EWCA Civ 2081, *Ellis v Chief Constable Essex Police* (2003) EWHC 1321.

[568] (2003) UKHL 53.

Human Rights (ECHR),[569] particularly the guarantee of the right to privacy. The Act required English courts to have regard to the ECHR in developing the common law.[570]

In 1991, the English Court of Appeal declared that:

> It is well known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person's privacy. The facts of the present case are a graphic illustration of the desirability of Parliament considering whether and in what circumstances statutory provisions can be made to protect privacy of individuals.[571]

By 2001 however, the same Court of Appeal was able to declare, in *Michael Douglas v Hello!* (No 2)[572] that:

> The courts have done what they can, using such legal tools as were to hand, to stop the more outrageous invasions of individuals' privacy; but they have felt unable to articulate their measures as a discrete principle of law. Nevertheless, we have reached a point at which it can be said with confidence that the law recognises and will appropriately protect a right to personal privacy.[573]

Two reasons were given for the change in outlook:

- Although the common law and equity grow by slow and uneven degrees, they are today in a position to respond to an increasingly invasive social

---

569 European *Convention for the Protection of Human Rights and Fundamental Freedoms* (1950). Hereafter ECHR .

570 S 6 UK Human Rights Act 1998.

571 Per Glidewell LJ in *Kaye v Robertson* (1991) FSR 62 (CA). See also Bingham L J's dictum in the same case that: "[t]his case nonetheless highlights, yet again, the failure of both the common law of England and statute to protect in an effective way, the personal privacy of individual citizens." The case involved Gorden Kaye, a well-known actor, who suffered life-threatening injuries in a car accident. Kaye attempted to obtain an order to restrain publication of photographs of the injuries he suffered in the crash. The photographs were obtained by deception through a tabloid journalist who entered the hospital and took the photographs while Kaye was undergoing treatment. A friend of Kaye was granted an interlocutory injunction preventing the editor (Anthony Robertson) and the newspaper (the Sunday Sport) from using the photographs. On appeal, the Court of Appeal reversed the lower court's decision.

572 2001 QB 967 (CA).

573 Ibid, per Sedley L J.

environment by affirming that everybody has a right to some private space.

- Secondly, "the Human Rights Act 1998 requires the courts of this country to give appropriate effect to the right to respect for private and family life set out in Article 8 of the European *Convention on Human Rights and Fundamental Freedoms*."[574]

In effect, English courts must not only take into account the jurisprudence of both the European Commission and the European Court of Human Rights which points to a positive obligation to respect privacy, they must also act in a manner compatible with the right to privacy and other Convention rights. By means of statutory intervention therefore, the common law and equity in England have been brought into conformity with the prevailing norms of international human rights law particularly as it concerns privacy.[575]

3.5 Expansion of the remedy for breach of confidence

English courts have used the equitable remedy of breach of confidence to protect information privacy.[576] In the *Wainwright*[577] case, the House of Lords advocated a pragmatic approach to the protection of privacy by means of incremental expansion of existing remedies to cover the circumstances presented by claims of breach of privacy.[578] The development of the law of confidence to accommodate privacy claims effectively began with the case of *Douglas v Hello*,[579] after the enactment of the Human Rights Act 1998.

---

574 Ibid, per Sedley L J.

575 See Lord Nicholls' minority judgment in *Naomi Campbell v MGN Limited* (2004) 2 AC 457 (HL).

576 Ibid. The House of Lords, per Lord Nicholls, noted that English courts have long afforded protection in the unlawful use personal information by means of the cause of action which became known as breach of confidence.

577 (2003) UKHL 53.

578 Lord Hoffmann asserted that privacy is not "capable of sufficient definition to enable one to deduce specific rules to be applied in concrete contexts"…and therefore any "perceived gap can be filled by judicious development of an existing principle." par 8.

579 (2001) 2 WLR 992 (CA) hereafter referred to as *Douglas No 1*.

The Act, by section 6 thereof, requires the courts to give effect to the ECHR which protects the right to privacy. Under the pragmatic and incremental approach favoured by the House of Lords, private information are increasingly being classified as "confidential" and thus subject to injunctive reliefs or damages. This was made possible, in the case where private information was involved, by relaxing the requirement to show a pre-existing confidential relationship and by the recognition that publication of private material in and of itself constitutes a "detriment".[580] The expansion of the equitable remedy of breach of confidence is seen as adequate in:

> …the great majority of situations, if not all situations, where the protection of privacy is justified, relating to events after the Human Rights Act 1998 came into force, an action for breach of confidence now will, where this is appropriate, provide the necessary protection."[581]

In the *Wainwright* case, although the House of Lords was unwilling to recognise a stand-alone tort of privacy, it nevertheless advocated the expansion of the remedy of breach of confidence in defence of the right to information privacy. In *Coco v AN Clark (Engineers) Ltd*[582] the requirements for the tort of breach of confidence were set out as follows:

- the information must have the necessary quality of confidence about it,
- the information must have been imparted in circumstances importing an obligation of confidence,
- there must be an unauthorised use or disclosure of that information to the detriment of the party communicating it.

English courts have overcome the conceptual difficulties inherent in applying these requirements to privacy claims by fundamentally expanding and adjusting their considerations of the requirements in actions for breach of privacy. What follows is a brief analysis of the said expansions and adjustments that were required to stretch

---

580 See *AG v Guardian Newspapers* (No 2) 1990) 1 AC 109. See also *Venables v News Group Newspapers* (2001) Fam 430.

581 Per Lord Woolf in *A v B Plc* (2003) Q.B. 195 at 205.

582 (1969) RPC 41, 47.

the tort of breach of confidence wide enough to accommodate breach of privacy.

3.5.1 "Information must have the necessary quality of confidence about it"

In relation to the requirement that the information must have the necessary quality of confidence about it, the English courts adopted the principle of "*reasonable expectation of privacy*". In determining whether a privacy breach has occurred, legal decisions in privacy enforcement cases frequently hinge on the issue of what constitutes a "reasonable expectation of privacy". The term is best explained by reference to case law where its application was elaborated.

In *Katz v United States*,[583] Federal Bureau of Investigation (FBI) agents in the US, acting without a warrant, placed electronic eavesdropping equipment on the outside of an enclosed telephone booth where Katz conducted his business. The American Supreme Court held that eavesdropping on Katz in this way violated his Fourth Amendment rights because he justifiably relied on the privacy of the telephone booth. The Court held that (a) an enclosed telephone booth is an area where, like a home a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic, as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment. In his concurring judgment, Justice Harlan outlined two requirements that must be present before a finding of reasonable expectation of privacy can be established: first that a person must have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[584]

In Europe, the balancing test of deciding when a privacy violation is necessary in a democratic society depends on the seriousness of the privacy violation. Breaches of privacy are allowed if they are necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country.[585] Although the notion of reasonable expectation of privacy does not play as fundamental a role in the European outlook on privacy as in the US, it is nevertheless

583 389 US 347 (1967).
584 Concurring opinion of Harlan J at 361. See also *Kyllo v United States* 33 U.S. 27 (2001).
585 Leenes and Koops 2005 (12) *Mich Telecomm & Tech L Rev* 127-128.

a factor in the consideration of the seriousness of alleged privacy violations.

In *Campbell v MGN Limited*,[586] Lord Nichols was of the view that the touchstone of private life is whether in respect of the disclosed facts, the person in question had a reasonable expectation of privacy. The crucial question to answer in determining whether there was a reasonable expectation of privacy is therefore, "what a reasonable person of ordinary sensitivity would feel if she was placed in the same position as the claimant and faced with the same publicity."[587]

3.5.2 "Obligation of confidence"

The requirement that the information must have been disclosed in circumstances that import an obligation of confidentiality means that some relationship must exist between the parties. It is the breach of this confidential relationship,[588] by publication to others, that courts of equity sought to prevent as such breaches were characterized as unconscionable.[589] Emphasis was thus on who published the private information; if it was by a person in fiduciary relationship with the complainant, such publication was deemed wrongful. As shown in the *Douglas (No 1)*[590] case, the emphasis on *who* published the offending material has now shifted to a consideration of *what* was published.[591] The new focus, with reference to privacy claims, makes it easier to examine the facts disclosed in the light of the protection of private life in the ECHR, whether there was a reasonable expectation of privacy.

---

586 (2004) UKHL 22.

587 Ibid per Lord Hope.

588 Confidential relationships may arise by express agreement between the parties or may be fiduciary relationships imposed by the law. See for example, the cases of *Duke of Argyll v Duchess of Argyll* (1967) 1 Ch 302; *W v Edgell* (1990) Ch 59 and *Attorney General v Guardian Newspapers* (1987)1WLR 1248.

589 *Stephens v Avery* [1988] Ch 449.

590 (2001) 2 WLR 992 (CA). See also *Venables v News Group Newspapers* (2001) Fam 430 and *Attorney General v Guardian Newspapers* (No 2) (1990) 1 AC 109.

591 See Morgan 2003 (62) *CLJ* 444.

3.5.3 "Unauthorised use or disclosure of information"

In respect of the third requirement, one of the fundamental obstacles in stretching a tort of breach of confidence to accommodate a claim for privacy invasion is that there must be an unauthorised use or disclosure of the information in issue, to the detriment of the party communicating it. It is well settled however, that the equitable remedy of breach of confidence does not regard intrusion as actionable. In the *Wainwright* case,[592] a mother and her son who went to see a relative in prison were strip-searched. Although the search resulted in the prison officials becoming acquainted with information of a personal nature relating to the mother and her son, the House of Lords held that there was no breach of privacy.

The fact that the prison officials did not publish the private details of the searches obviously worked against a claim for privacy. However, dicta in the *Campbell* case, that intrusion into privacy could by itself constitute a detriment, affords opportunity to bring a claim for breach of information privacy by means of an action for breach of confidence.[593] Information privacy concerns an individual's control over the acquisition, disclosure and use of personal information. This type of privacy is breached by the acquisition of otherwise private information by a second or third party and signifies a loss of control over information.

While breach of confidence relies on disclosure, information privacy on the other hand, depends on individual autonomy which must contend with not only disclosure of information, but also intrusion. The expansion of the requirement for breach of confidence to accommodate intrusion, in addition to disclosure, in *Douglas v Hello!*[594] made it possible for the protection of privacy under the action for breach of

---

592 (2003) UKHL 53.

593 In the Campbell case, Lord Nicholls said: "An individual's privacy can be invaded in ways not involving the publication of information. Strip searches are an example. The extent to which the common law as developed thus far in this country protects other forms of invasions of privacy is not a matter in the present case." (2004) UKHL 22 at par 15.

594 (2001) 2 WLR 992 (CA). According to Sedley J at par 126:

> What a concept of privacy does, however, is accord recognition to the fact that the law has to protect not only those people whose trust has been abused but those who simply find themselves subjected to an unwanted intrusion into their personal lives. The law no longer needs to construct an artificial relationship of confidentiality between intruder and victim: it can recognise privacy itself as a legal principle drawn from the fundamental value of personal autonomy.

confidence.

3.5.4 The position in Nigeria today

While the English common law has developed to the point where it now recognises the right to privacy and protects same by means of the remedy of breach of confidence, the same cannot be said for the common law in Nigeria today. There is no discernible judicial or statutory policy to afford a robust privacy rights protection. The development of the law of privacy in England was given statutory impetus with the enactment of the Human Rights Act of 1998. Although there is no such statute in Nigeria, there is nonetheless the Bill of Rights guaranteed in the 1999 Constitution. The right to privacy guaranteed therein has so far failed to inspire the development of the tort of privacy. Some of the reasons for this failure were highlighted in the previous chapter.

The question that arises is whether Nigerian courts should take a cue from the developments in England and begin to expand the jurisprudence relating to breach of confidence as a starting point in protecting information privacy. In taking such a step, the courts would have to overcome the hurdle of the requirements that ground the remedy of breach of confidence. The foregoing analysis of the development in the UK shows the track Nigerian courts may have to follow in order to adapt the equitable action for breach of confidence in aid of information privacy protection. The courts would have to adopt the fundamental changes in the "new" law of confidence highlighted above. One argument in favour of adopting the action for breach of confidence in protecting information privacy is that it is more precise, well established and provides a more doctrinally sound basis for developing remedies for information privacy breaches.[595]

This is in contrast to any proposed stand-alone tort of privacy that will be subject to definitional and doctrinal imprecision. It is debatable however, whether the extension of the law of breach of confidence to protect information privacy will fit the peculiar circumstances of the Nigerian environment. Moreover, the pragmatic and incremental approach of the English courts in this branch of the law stems from the

595 Wacks 1980 (96) *LQR* 73.

obligations imposed by the Human Rights Act to give effect to European Convention rights.[596] There is no equivalent statute as the English Human Rights Act in Nigeria. Rather than adopt the remedy of breach of confidence to address information privacy issues, it is better to develop a proper statutory framework for the protection of information privacy. This will avoid the conceptual distortions inherent in the artificiality of the breach of confidence approach. One of the distortions relates to the traditional definition of breach of confidence which relies on the existence of a confidential relationship. The confidence that underpins the relationship is breached if one of the parties discloses private information to a third party.[597]

Information privacy breaches however, are more likely to be perpetrated by a stranger to the person whose privacy is compromised than a person in a close or fiduciary relationship with him. If a relationship can be construed to accommodate privacy, even when no relationship exists between the parties, a key element of the traditional requirements of the tort of breach of confidence is done away with.

The strict constructionist approach of many Nigerian judges may not accommodate the judicial "sleight of hand" required to stretch the action for breach of confidence to cover breach of information privacy.[598] This constraint will hinder the development of binding case law that can protect the processing of private information in Nigeria. Furthermore, and with particular reference to the EU Directive on data protection, it has been argued that on the face of the provisions of the Nigerian Constitution,[599] "only Nigerian citizens have enforceable claims to the 'fundamental right to privacy' since the operative word in the constitutional provision is 'citizens' either by birth, registration or naturalisation."[600] Although this argument has not received any judicial stamp of authority, it raises the question whether EU citizens can avail themselves of even the limited scope of information privacy protection available in Nigeria.

---

596 S 6 Human Rights Act 1998.

597 According to Lord Griffiths, the jurisdiction in confidence "…is based not so much on property or on contract as on the moral principles of loyalty and fair dealing." See *A.G. v Guardian Newspaper* (No 2) (1990) 1 AC 109 at 269.

598 See Nwabueze 5th Sept 2006 *The Guardian* 69.

599 S 37 Constitution of the Federal Republic of Nigeria, 1999.

600 Kusamotu 2007 (16) *Info & Comm Tech L* 154.

3.5.5 Conclusion

Essentially, the protections in the statutes discussed above are concerned more with the confidentiality of information in the possession of government or particular agencies of government than with data protection. Furthermore, these Acts do not address the private sector of the economy where the Internet and other network service providers operate. The collection of personal information in this sector is not regulated.[601]

In the private sector, the banking sector has been more pro-active by adopting varying degrees of security and confidentiality measures on a voluntary basis,[602] in some cases reinforced by advisory codes of practice for the sector.[603] However, in the absence of a statutory framework for the protection of information privacy, dispute resolution under an industry-defined code of ethics which is not readily available to the public, will revert to the extant banking laws and other common law remedies. These remedies are of a general nature and do not meet the demands of the new digital medium.

Furthermore, the private sector initiatives do not provide a uniform, comprehensive,

---

601 The Computer Security and Critical Information Infrastructure Protection Bill (2005) was the first legislative attempt to regulate the activities of Internet service providers as well as other network service providers. S 12 of the proposed legislation deals with data retention and illegal interception of data. Between 2005 and 2010, up to six different Bills dealing with Cybercrime and security have been submitted to the National Assembly. The Bills are: Computer Security and Critical Information Infrastructure Protection Bill 2005 (sponsored by the Executive); the Cyber Security and Data Protection Agency (Establishment, etc) Bill 2008 (sponsored by Hon. Bassey Etim); the Electronic Fraud Prohibition Bill 2008 (sponsored by Senator Ayo Arise); the Nigeria Computer Security and Protection Agency Bill 2009 (another executive bill); the Computer Misuse Bill 2009 (sponsored by Senator Wilson Ake) and the Economic and Financial Crimes Commission Act (Amendment) Bill 2010 (sponsored by Hon. Abubakar Shehu Bunu). None of the Bills has been enacted into law. See Nkanga 31st March 2011 *Thisday*. A seventh Bill, the Cybersecurity Bill, 2011 (an Executive Bill) has been approved by the government for submission to the National Assembly.

602 Many of the banks have adopted privacy policies that seek to protect customers' information privacy. See for example, Zenith Bank's *Privacy Policy* [online].

603 See Central Bank of Nigeria *Guidelines on Electronic Banking* 10 [online]. The guidelines provide, *inter alia*, that banks should protect the privacy of the customer's data by ensuring:

- that customer's personal data are used for the purpose for which they are compiled
- consent of the customer must be sought before the data is used
- data user may request, free of cost for blocking or rectification of inaccurate data or enforce remedy against breach of confidentiality
- processing of children's data must have the consent of the parents and there must be verification via regular mail.
- strict criminal and pecuniary sanctions are imposed in the event of default.

data protection regime. Even the Central Bank's guidelines[604] do not specify the protocols to be followed by governmental agencies and the banks in accessing a customer's banking records or where external associates or subsidiaries of the banks seek access to customer banking records. Nor does it deal with the issue of banks selling customer banking records for marketing purposes. In any event, the guidelines are just that – guidelines, without any coercive enforcement provision or mechanism. Even if the guidelines were to be backed by criminal liability enforceable against an erring bank, an individual that is adversely affected by the wrongful act of a bank will not have a legally enforceable right under the guidelines against such a bank or any other party responsible for a breach of his privacy.

What the EU *Directive* envisages in respect of a third country, is a legal framework consisting of laws and regulations that adequately protect the data privacy of its citizens and therefore able to assure the same protection for EU citizens whose data are transferred to such third country. Since the EU *Data Protection Directive* came into force, the European Commission (EC) has approved a number of third countries as having adequate levels of data protection. For example, in the case of Switzerland, the European Commission (EC), on July 26, 2000, issued its decision declaring that Switzerland's laws provide an adequate level of protection governing the transfer of private data.[605] The EC report noted that Switzerland's judicial systems at the federal and cantonal levels have developed binding case law that protects "the quality of the data processed, the right of access of the persons concerned, and the right to request the correction or destruction of data."[606] Nigerian jurisprudence does not at present have such binding case law regarding privacy. If the judicial framework in Nigeria with its lack of a developed case law protecting private information is not adequate to protect its own citizens, it is unlikely to be found adequate to protect EU citizens.

A better option would therefore be to create a statutory tort of privacy that would cover all persons whose data are used in the country. A specific statutory framework such as a Data Protection Act, that will protect information privacy is not only

---

604 Ibid.

605 European Commission *Decision 2000/518/EC, art 1 (2000) O J (L 215).*

606 Ibid.

necessary, but will give impetus to the country's national IT and outsourcing policy aspirations.[607]

3.6 Constitutional protection of the right to privacy

3.6.1 Introduction

The Nigerian constitution emphasizes the dignity of the human person[608] and one of the ways it seeks to protect that dignity, is through the guarantee of the right to privacy. The protection of the dignity of the Nigerian person accords with the UDHR and the communal nature of the Nigerian society that places great premium on the dignity of man.[609] Article 12(1) of the UDHR[610] outlines the right to privacy in the following terms:

> 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 above article of the UDHR has been incorporated in the Nigerian Constitution[611] in section 37 which provides as follows:

> The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and

---

607 Ibid n 421. Chapter 16(xxiii) of the Nigerian *National Policy for Information Technology* provides for the enactment of a Data Protection Act (DPA) for safeguarding privacy of national computerised records and electronic documents. While no specific recommendation is contained in the outsourcing policy document for data protection legislation, it is assumed that the proposed DPA will cover all activities dealing with private data in Nigeria. See *National Outsourcing Policy and Institutional Framework for Nigeria* 2007.

608 S 34 Constitution of the Federal Republic of Nigeria 1999. According to Howard, the African concept of human rights is actually a concept of human dignity. It is what defines "the inner (moral) nature and worth of the human person and his or her proper (political) relations with society." See Howard and Donnelly 1986 (80) *Am Polit Sci Rev* 802.

609 See n 521.

610 See also a 17 of the *ICCPR*.

611 See n 607. S 12 (2) of the Nigerian Constitution empowers the National Assembly to "make laws for the Federation or any part thereof with respect to matters not included in the Exclusive Legislative List for the purpose of implementing a treaty". .Nigeria has had a long history of constitutional protection of privacy starting in 1960 with S 22 Constitution of the Federation of Nigeria, 1960; s 23 Constitution of the Federal Republic of Nigeria, 1963; s 34 Constitution of the Federal Republic of Nigeria, 1979, Constitution of the Federal Republic of Nigeria, 1989 and Constitution of the Federal Republic of Nigeria, 1993.

protected.

One aspect of privacy that is protected in the above section is the inviolability of the private home of a citizen or other inhabitants of Nigeria. Although the reference is to the home, the protection primarily avails the person who dwells in the home and the right is not dependent upon a property right in the home. What this aspect seeks to achieve is the protection of an individual's solitude and seclusion from the observation of other members of the society.[612] This is particularly important in ensuring the dignity and freedom of a family to engage in the intimacies of marital and family life without observation or interference by outsiders.[613]

The *African Charter on Human and People's Rights* provides that "[t]he family shall be the natural unit and basis of society. It shall be protected by the State..."[614] Although Nigeria is a party to the Charter, in Nigeria however, individuals, families and/or communities have often by forced evictions, been removed from the homes and/or land they occupy, thereby subjecting the affected people to arbitrary or unlawful interference with their privacy, family or home.[615]

The very notion of private property (which is protected in section 43 of the

---

612 Westin *Privacy and Freedom* 31-32.

613 Ibid. This is the state of intimacy, in which according to Westin 31, the individual is acting as part of a small unit that claims to exercise corporate seclusion so that it may achieve a close and frank relationship between two or more individuals..

614 See a 18(1).

615 According to the US State Department *Annual Human Rights Report 2005* on Nigeria [online],

> Throughout the year the Federal Capital Development Authority (FCDA) continued to demolish homes and businesses in the Federal Capital Territory (FCT). Thousands of homes in the suburbs of Karmo, Kado, and Lugbe were deemed illegal squatter settlements and bulldozed. In April the FCDA bulldozed some 400 houses, small hotels, and other businesses in the middle-class suburb of Kubwa. On April 27, the House of Representatives passed a resolution ordering an end to the demolitions, claiming that many houses had been approved by the FCDA or previous FCT ministers. The Abuja high court also issued an injunction on the FCT Minister to stop further demolition, which he rejected on grounds that the high court only had jurisdiction if there had been a lower court decision. In September businesses in two high rent districts of Abuja were demolished, as was a police station in Lugbe. On November 28, the government announced that about 1,500 houses in Chika had been bulldozed, leaving an estimated 10 thousand people homeless; however, observers estimated that 2 square miles of dense one-story housing had been bulldozed, leaving some 95 percent of the estimated 500 thousand residents homeless. Although the FCT Minister announced in November that the demolitions would finish by December, the demolitions continued at year's end. See US State Department *Annual Human Rights Report 2005* [online].

Constitution) affords another means of protecting privacy in so far as it denotes a relationship between persons in relation to things. By referring to a thing as private property, it establishes an exclusive relationship between the owner of the private property and all others in relation to that thing. This right to exclude others, so inherent in the concept of property, affords another means of privacy protection.[616]

The reference to correspondence, telephone conversations and telegraphic communications indicate a clear intention to protect information privacy. Information privacy is a specific instance of privacy which involves a person's right against unlawful interference in relation to information held by others about him or her. In particular, the scope of information privacy covers the collection, processing, storage, use and disclosure of personal information by public as well as private bodies. The constitution protects the privacy right in personal information by limiting the ability of people, organisations and the government to gain, publish, disclose or use information about others.

3.6.2 The protection of fundamental rights

Because privacy is a fundamental human right, it is necessary to look at the way Nigerian courts have responded to other human rights breaches in the past. This will give an insight to how the courts may likely respond to alleged breaches of privacy today. This is all the more necessary because of the paucity of cases dealing strictly with the right to privacy in Nigeria. Some of the few privacy cases will be examined in paragraph 3.4.2 hereunder but first, an overview of the legal system and judicial process in Nigeria.

3.6.2.1 A brief overview of the legal system

The Nigerian legal system is composed of English common law, customary law and sharia law in the northern states of Nigeria. Nigerian jurisprudence derives from a variety of sources, including:[617]

---

616 Law Reform Commission of Ireland *Report* 44 [online].

617 Obilade *The Nigerian Legal System* 55-56.

- Nigerian Legislation
- English law,[618] consisting of the received English law (comprising the common law; the doctrines of equity; statutes of general application in force in England on January 1, 1900; Statutes and subsidiary legislation on specific matters) and English law made before October 1, 1960 and extending to Nigeria.
- Customary Law
- Judicial precedents

Provisions of military decrees and international conventions have been incorporated into Nigerian Law. Nigerian customary law is largely unwritten and in order for a customary law to be valid in the case in which it is applied, it must be compatible with natural justice, equity and good conscience - the repugnancy test.[619] Sections 33 through to 42 of the 1999 Constitution of the Federal Republic of Nigeria provide for a broad range of rights and freedoms.

The judicial powers exercised by the various courts are vested in them by the 1999 Constitution which established them.[620] The courts are the Supreme Court,[621] Court of Appeal,[622] the Federal High Court,[623] High Court of the Federal Capital Territory,[624] State High Courts,[625] Sharia Court of Appeal of the Federal Capital

---

618 See s 2 Law (Miscellaneous Provisions) Law (Laws of Lagos State, Cap 65 1973); s 28 High Court Law (Northern Nigeria Laws 1963, Cap 49); s 3 Law of England (Application) Law (Western Region of Nigeria Laws 1959, Cap 60); s 15 High Court Law (Eastern Nigeria Laws 1963, Cap 61); s 28 Interpretation Act No 1 of 1964.

619 In *Eshugbayi Eleko v Officer Administering the Government of Nigeria* (1931) A.C. 662 at 673, Lord Atkin expressed the view that a "barbarous" custom must be rejected on the ground of repugnancy to natural justice, equity and good conscience.

620 S 6(1) Constitution of the Federal Republic of Nigeria 1999, vests judicial powers of the Federation "in the courts to which this section relates, being courts established for the Federation." s 6(6) also vests powers in state courts established by the constitution.

621 Id at s 230.

622 Id s 237.

623 Id s 249.

624 Id s 255.

625 Id s 270.

Territory[626] and Customary Court of Appeal.[627] It was in the 1979 Constitution that, for the first time, judicial powers were vested in the courts by the Constitution. As noted by Eso, J.S.C., in reference to the 1979 Constitution, "this is the first time in the history of the country that the Constitution has specifically vested judicial powers of the Federation in the courts."[628]

3.6.2.2 Fundamental rights and the judicial process

The human rights which the courts are empowered by the Constitution to protect can be roughly divided into two categories. In the first category are those rights, the protection of which, the court is called upon to determine primarily, the right of the individual. The rights in this category are said to be "self-directing rights".[629] These are rights which can be enforced by substantive actions. Such actions are founded on those fundamental rights which may not be restricted as the Legislature pleases,[630] or if restricted at all, it is done under emergency powers during a declared state of emergency.[631]

The second category of cases involves procedural fundamental rights which must be observed whenever the occasion for their observance arises. An example of such right is the right to a fair hearing.[632] In this second category of cases, the right of the individual, important as it is, is not the only interest demanding recognition. The rights involved here are those which may be subject to some restrictions by the Legislature. In this category, there are rights such as the right to private and family

---

626 S 260.

627 See s 265.

628 Eso *Thoughts on Law and Jurisprudence* 30. It was under the 1979 Constitution that judicial powers of the federation were for the first time spelt out and vested in the various courts created by the Constitution (see fn 438 above). Previous Constitutions merely established the Supreme Court and High Court for the Federal Capital Territory while the various regional constitutions established High Courts for their regions. See also *Bronik Motors Ltd v Wema Bank* (1985) 6 NCLR 1.

629 *Nemi v State* (1994) 9 NWLR Pt 366 1; see also *Tukur v Govt of Gongola State* (1989) 4 NWLR Pt. 117 517; *Achebe v Nwosu* (2003) 7 NWLR Pt. 818 103 at 130 par A-D and Grove 1963 (7) *JAL* 152-171.

630 Eg s 34 (right to dignity), s 44 (right to compensation for compulsory acquisition of property).

631 See s 33 (right to life), s 35 (right to personal liberty) and s 42 (right to freedom from discrimination).

632 S 36.

life (right to privacy),[633] freedom of expression,[634] freedom of movement[635] and right to peaceful assembly and association.[636] Under this category of cases, it is taken that the right of the individual has been breached; the question that the court has to determine is whether the breach is justifiable or not. In doing so, the court must take into account the greater interest of the society or community at large.

The rights are not absolute; they are subject to restrictions which must be "reasonably justifiable in a democratic society".[637] For example, the right to freedom of expression may be restricted by the state in order to preserve public order. In *D.P.P v Obi*[638] the Supreme Court of Nigeria was called upon to consider the validity of the sedition laws contained in sections 50 and 51 of the Criminal Code in the light of section 24 of the 1960 constitution which guaranteed freedom of expression. It was argued on behalf of the accused that sections 50 and 51 of the Criminal Code were inconsistent with the provisions of section 24 of the Constitution. The Supreme Court held, in relation to the clause in section 24(2) of the Constitution which imports the "reasonably justifiable" requirement, that it is reasonably justifiable in a democratic society to take reasonable precautions to preserve public order.

3.6.2.3 The courts, the individual and the state

Cases in the second category of rights are often more difficult to determine because they usually require the courts to examine matters of public policy. It has been said that Commonwealth judges approach cases dealing with the rights and liberties of the individual as they do any other legal problem, by applying the ordinary methods of logical deductions.[639] As a result, there is often a failure to adequately address the

633 S 37.

634 S 39.

635 S 41.

636 S 40.

637 S 45.

638 (1961) 1 All NLR 186. See also *R v Amalgamated Press Ltd* (1961) 1 All N.L.R. 199 at 201-2. The same court affirmed the constitutionality of the sedition laws.

639 Nwabueze *Role of Judiciary in the Conflict between Freedom of the Individual and the State Power*.

question of choice between the right of the individual and that of the state and the role of the court in striking a balance between the freedom of the individual and the right of the state to preserve itself.[640] The period just after Nigeria's independence was characterized by conservative judicial self-restraint; the judges of the period, having been schooled in the colonial judicial traditions, often regarded matters of public policy as outside their scope.[641]

Nevertheless, judicial restraint did not mean an abdication of judicial responsibility to act as sentinels of the rights of the people. In *Cheranci v Cheranci,*[642] the High Court of the then Northern Region of Nigeria was asked to declare sections 33 - 35 of the Northern Region Children and Young Persons Law[643] void by reason that they breached the rights of the defendant to freedom of expression, peaceful assembly and association and conscience. The relevant sections complained of make it a crime to indoctrinate and encourage children and young persons in political activities.

The trial judge found as proven facts, that the rights of the defendants to freedom of expression and peaceful association and assembly, but not freedom of conscience, had been violated by the laws complained of. The question that then arose was whether the said laws were "reasonably justifiable in a democratic society". The fact that the law had been passed by the legislature of the Northern Region was, according to the judge, merely indicative of its reasonable justifiability. He, however, sought to determine if indeed it was, and what the phrase "reasonably justifiable in a democratic society" meant, for as he said:

> It is the duty of the judges to determine fully the constitutionality of an impugned enactment. For this, they must, after considering all the

---

640 Ibid.

641 See Brett F J in *Director of Public Prosecution v Chike Obi* (1961) 1All NLR. 188 at 197:
> The Constitution entrusts the courts with the task of deciding conclusively whether or not any legislative measure contravenes Chapter III of the Constitution, and I do not wish to anything which might suggest that the courts are evading their responsibilities. Nevertheless, it is right that the courts should remember that their function is to decide whether a restriction is reasonably justifiable in a democratic society, not to impose their own views of what the law ought to be.

642 (1960) NRNLR 24.

643 NR No 28 of 1958.

> relevant factors, rely on their own judgment. It does not necessarily follow that because the legislature has passed a law that every provision of a law is reasonably justifiable. The courts have been appointed sentinels to watch over the fundamental rights secured to the people of Nigeria by the Constitution Order and to guard against any infringement of those rights by the state. If the courts are to be effective guardians, then the judges must not only act with self-restraint and due respect for the judgment of the legislature, but they must also use their own impartial judgment without undue regard for the claims either of the citizen or of the state.[644]

The judge formulated two principles to guide him in determining whether a restriction upon a fundamental right can be said to be reasonably justifiable in a democratic society. The principles are:

(1) There is a presumption that the Legislature has acted constitutionally and that the laws which they have passed are necessary and reasonably justifiable.
(2) A restriction upon a fundamental right must, before it may be considered justifiable –
    a. be necessary in the interest of public morals or public order, and
    b. must not be excessive or out of proportion to the object which it is sought to achieve.[645]

In examining the facts of the case against the principles formulated, he was of the view that the presumption of constitutionality of the law complained of imposed on the defendant the burden to prove that the law was not reasonably justifiable. The defendant, the judge concluded, had not discharged that burden. The law was therefore reasonably justifiable in the interest of public order and morality. As said, the right to privacy falls within the second category of rights. It is therefore not an absolute right and is subject to derogations allowed by the Constitution.[646]

---

644 Per Justice Bate in *Cheranci v Cheranci* (1960) NRNLR 24 at 28.

645 Id at 29. See also the case of *Folatalu v A-G Solomon Islands* (2003) CHR 279 at 301 where the High Court of the Solomon Islands referred to the above principles.

646 S 45 Constitution of the Federal Republic of Nigeria 1999.

3.7 Judicial protection of the right to privacy

3.7.1 Introduction

Nigerian courts have the constitutional duty to determine the scope of the privacy right and whether it has been breached.[647] Not many court actions have been instituted in the country to test the scope of the constitutional protection of privacy. The few that have been decided by the courts have mostly failed on technical grounds without the courts actually deciding the merits of the claim to privacy.

The actions have failed because the principal claims sought, being claims grounded in the common law, were joined with an ancillary claim that discloses a breach of the right of privacy.[648] The courts in Nigeria have been quick to point out that where the principal reliefs sought in an action under the Fundamental Rights (Enforcement Procedure) Rules[649] are tortious in nature, the action is incompetent. Claims in tort are maintainable only by following the common law procedure of causing a writ of summons to be issued against the offending party.[650]

For a claim to qualify as falling under a fundamental rights claim, it must be clear that the principal relief sought is for the enforcement, or for securing the enforcement, of a fundamental right. The jurisdiction conferred by section 46(1) of

---

647 Id s 6.

648 See *J S Olawoyin v Att-Gen Northern Region* (1961) 1 All NLR. 269; *Ransome-Kuti v Att.-Gen of the* Federation *& Ors* (1985) 16 NSCC (Pt. 1) 879; *Madu v Neboh & Anor* (2002) 2 CHR 67.

649 See *Abdulhamid v Akar* (2006) All F.W.L.R. (Pt. 321) 1191; see also *Onwo v Oko & Ors* (1996) 6 N.W.L.R. (Pt. 456) 584 at 603; *Ogugu v The State* (1994) 9 NWLR (Pt. 366) 1.

650 Section 46(3) of the 1999 Constitution provides as follows:

> The Chief Justice of Nigeria may make rules with respect to the practice and procedure of a High Court for the purpose of this section". Pursuant to this provision, the former Chief Justice of Nigeria, Hon. Justice Idris Legbo Kutigi made rules for the practice and procedure of the High Courts of Nigeria known as the Fundamental Rights (Enforcement Procedure) Rules 2009 for speedy adjudication of cases involving the fundamental rights of Nigerians. The Fundamental Rights (Enforcement Procedure) Rules 2009 which came into force in November 2009 repealed and replaced the Fundamental Rights (Enforcement Procedure) Rules, 1979 which were made pursuant to the 1979 Constitution. The 2009 Rules simplified the process of seeking redress by removing some of the judicial bottlenecks that made the 1979 Rules burdensome for litigants and lawyers. For a claim to qualify as falling under fundamental rights claims, it must be clear that the principal relief sought is for the enforcement of a fundamental right. Thus, where the alleged breach of fundamental right is incidental to the substantive claim which is of a common law nature, it will be incompetent.

the 1999 Constitution is in respect of any person who alleges that any of the provisions of chapter IV of the Constitution "has been, is being or likely to be contravened."[651] It follows therefore, that an action seeking to enforce the fundamental right to privacy guaranteed under section 37 of the 1999 Constitution must be filed strictly as a stand-alone claim for the enforcement of the right to privacy under the procedure set out in the *Fundamental Right (Enforcement Procedure) Rules*. Thus, the principal relief and any ancillary relief sought must not be incidental to a claim under tort, contract or administrative law for example.

3.7.2 Privacy protection in Nigerian case law

3.7.2.1 Ransome-Kuti v Att-Gen of the Federation & Ors

Of the few cases dealing with privacy rights, perhaps the most controversial is the case of *Ransome-Kuti v Att-Gen of the Federation & Ors*[652]. The plaintiffs sued the Federal government for the willful destruction of their building and chattels, assault and battery by soldiers of the Nigerian Army. The claim, though grounded in tort, also invoked chapter III of the 1963 Constitution which then was the Bill of Rights guaranteeing fundamental rights. In the suit, the Attorney-General of the Federation, along with other public officers, was sued as representing the government of Nigeria. At the trial court, the case proceeded on the basis of a claim in tort. The trial judge held that no action lay against the Attorney-General as a representative of the government for a wrong committed by its servants. Being grounded in common law, the High Court held that the state enjoyed immunity from legal action and could not be sued in its own court for the tortious acts of its servants.

The Court of Appeal and the Supreme Court upheld the decision of the High court, holding that the government enjoyed state immunity. The fundamental right referred to in the claim of the plaintiffs was the right to private and family life under section 23 of the 1963 Constitution which is essentially the same provision as in section 37 of the 1999 Constitution. While noting the plaintiffs/appellants invocation of the

651 *Abdulhamid v Akar* (2006) All FWLR (Pt 321) 1191 at 1209 par G-H. S 46 of the 1999 Constitution is a re-enactment of s 44(1) of the 1979 Constitution. The section seeks to make the hearing of human rights cases speedier than other civil cases.

652 (1985) 2 NWLR (Pt 6) 211.

fundamental rights provision of the Constitution, the Supreme Court refused to apply the said provision because they were merely referred to in the pleadings and not invoked as a substantive claim.[653] Arguably, the invasion of the plaintiff's premises, the forcible removal and acts of violence to the persons of some of the dwellers as well as other acts prejudicial to the quiet enjoyment of their home constitute violations of their rights to private and family life, particularly the inviolability of their home. The fact that the Supreme Court did not see its way clear to do substantial justice in the light of the wanton destruction of property and abuse of the fundamental rights of the plaintiffs in this case remains controversial.

3.7.2.2 J S Olawoyin v Att-Gen Northern Region of Nigeria

In *J S Olawoyin v Att-Gen Northern Region of Nigeria,*[654] the plaintiff sought a declaration that Part VIII of the *Children and Young Persons Law*[655] had been invalidated by the provisions of sections seven, eight and nine of the Sixth Schedule of the Nigeria (Constitution) Order in Council, 1954. Part VIII of the said law prohibited political activities by juveniles and made it a crime to induce children and young persons to engage in political activities. The Sixth Schedule of the 1954 Constitution made provisions for the protection of the fundamental rights to private and family life, freedom of association and conscience and freedom of expression. These were the rights the plaintiff alleged were violated by Part VIII of the *Children and Young Persons Law*.

The claim was dismissed on the ground that no right of the plaintiff was alleged to have been violated.[656] On appeal to the Supreme Court,[657] it was held that a person

---

653 Ibid. According to the Court, the mere reference to provisions of the Bill of Rights was not sufficient to ground a claim for the enforcement of fundamental rights, particularly in the circumstances of this case where the claim was filed and argued as a claim in tort. According to Justice Eso, "The plaintiff must be known to be seeking that redress and not merely calling in aid constitutional provisions in his action for damages" (232-233).

654 (1961) 1 All NLR. 269.

655 Northern Region Law No 28 of 1958.

656 The plaintiff did not have legal standing to sue (*locus standi*). Briefly stated, *locus standi* denotes the legal right to bring an action before a court of law. The plaintiff must show sufficient connection to, and harm arising from the act complained of. See *Adesanya v President of Nigeria* (1981) 1 All NLR 1 A fundamental flaw in the concept is that it focuses attention on the party seeking redress and not on the remedy he seeks. For a fuller discussion of the problem of *locus standi* in Nigerian jurisprudence, see

seeking a judicial declaration to invalidate a law must show that he is in imminent danger of coming in conflict with the law or that there has been real or direct interference with his normal business or other activity. It was argued for the plaintiff that he had children whom he wished to educate politically; the effect of the law would be to render any such action on his part illegal. The right to private and family life as guaranteed in the Constitution denotes the freedom to bring up one's children as one sees fit, including teaching them one's political beliefs. Unfortunately, the question whether the law complained of actually breached plaintiff's right to private and family life was not determined.

3.7.2.3 Cletus Madu v Neboh & Anor

In *Cletus Madu v Neboh & Anor,*[658] the plaintiff sought the enforcement of his fundamental right to privacy and claimed damages for unlawful and humiliating ejection from his home. Unlike the case of *Ransome-Kuti*[659] discussed above where the case proceeded mainly as a claim in tort but with reference to the right to private and family life, the claim in this suit proceeded in the High Court:

> For an order of the Honourable Court enforcing the Applicant's Fundamental Rights by restraining the Respondents, their servant, agents and privies from denying and continuing to deny the Applicant his right of privacy on (sic) guaranteed by section 34 of the constitution of the Federal Republic of Nigeria 1979 as amended.[660]

The facts of the case disclosed that the first defendant was the landlord of the Plaintiff, while the second defendant was first defendant's son. The second defendant forcibly removed the door to the plaintiff's room while plaintiff was away on a journey. The plaintiff lived with his sister who was forced to flee the premises as a result of the insecurity created by the removal of the door. Plaintiff alleged that he lost some money and other valuable property thereby. In support of his claim, the

---

Ogowewo 1995 (39) *JAL* 1-18.

657 See Aihe and Oluyede *Cases and Materials on Constitutional Law in Nigeria* 147.

658 (2002) 2 CHR 67.

659 (1985) 2 N.W.L.R. (Pt 6) 211.

660 See n 658 at 74 par E-F.

plaintiff filed an affidavit in which he annexed a copy of the tenancy agreement between himself and the first defendant. His counsel argued the case as a claim for the enforcement of fundamental rights for breach of privacy. However, after reviewing the affidavit evidence of both parties, the trial judge concluded that:

> As Exhibit A – tenancy agreement encapsulates the rights of the parties, and having regard to the fact that the facts therein are not within the contemplation of section 34 of the 1979 Constitution and the alleged violation, being of the tenant's rights within Exhibit A and not section 34, I hold the view that this action must fail.[661]

On appeal by the plaintiff, the Court of Appeal held that from the facts disclosed by affidavit evidence, the plaintiff/appellant's complaint was the damage done by the second respondent to his room in his possession by removing the door. The action of the respondent amounted to an unjustifiable interference with the room in the plaintiff's possession and that gave rise to an action in trespass.[662] The court was of the view that the dominant element in the wrong alleged by the plaintiff/appellant was the infringement of his right to an undisturbed possession of his room. According to Justice Olagunju, "[t]he interference with the right to enjoy family life arising from the positive act of trespass is, in my view, incidental."[663] Thus, whatever acts of invasion of privacy were disclosed in the action of the respondent did not bring the suit under section 42 of the Constitution.[664] Because the case was brought under the *Fundamental Rights (Enforcement) Procedure Rules*[665] inappropriately, the appeal was dismissed.

In none of the cases highlighted above did the courts determine on the merits, the scope and extent of the right to privacy that the Constitution guarantees. The attitude of the courts concerned, that is, the High court, the Court of Appeal and the

---

661 See n 658 at 76 par A-B.

662 See n 658 at 86 par G-H.

663 See n 658 at 88 par B-D.

664 Constitution of the Federal Republic of Nigeria 1979.

665 The Fundamental Rights (Enforcement) Procedure Rules were first formulated by the then Chief Justice of Nigeria under section 42(3) of the 1979 Constitution.

Supreme Court, indicates, as Nwabueze has suggested, an unduly logical approach to the resolution of the conflicts between the individual and the state on the one hand, and between individuals on the other.[666] This approach, in many cases, fails to strike a balance between the need of society to protect itself and the need of the individual in that society to assert his or her right. The result is that the amplitude of the rights guaranteed under the Constitution for the benefit of the citizens is sometimes denied them by reason of judicial constructs such as *locus standi,* which restrict access to judicial remedies.

3.7.2.4 Medical and Dental Practitioners Disciplinary Council v Dr. John E. N. Okonkwo

One case that may give an idea of how the courts might in future deal with cases relating to privacy right issues is the case of *Medical and Dental Practitioners Disciplinary Council v Dr. John E. N. Okonkwo.*[667] The Respondent, Dr. Okonkwo was tried by the disciplinary organ of the medical and dental practitioners association on a charge of infamous conduct. He was alleged to have violated the medical code of ethics that requires a medical practitioner to always take measures that will preserve life. The doctor was faced with a patient's refusal to give informed consent to a life-saving medical treatment, in this case, blood transfusion. The patient and her spouse were practicing Jehovah's Witnesses whose religious beliefs forbade them from accepting a blood transfusion even if such refusal would result in death. Knowing that the doctor was also a Jehovah's Witness, the patient and her spouse chose to receive treatment in his clinic. The patient's condition became critical; she required a blood transfusion as part of the medical procedure for managing her treatment. Her husband was informed of her condition and the need for blood transfusion. In very clear terms, he objected to the transfusion even though the consequences were made known to him.

The doctor respected the husband's religious beliefs and decision not to accept the recommended course of treatment and in the end, the patient died. At the trial, it was argued on behalf of the doctor that the dead patient and her spouse had a

666 See n 639.

667 (2001) 3 S.C. 92.

Constitutional right to object to the course of treatment recommended by the doctor. The disciplinary tribunal found the doctor guilty as charged whereupon he appealed. The Court of Appeal upheld his appeal and overturned the ruling of the tribunal. Not satisfied with the decision, the Disciplinary Council appealed to the Supreme Court. A judicial consideration and pronouncement on the merits of the scope of the right to privacy was made. As earlier stated, one of the grounds on which the decision of the tribunal was contested was that the dead patient and her spouse had a Constitutional right to object to the treatment on religious grounds. The right was founded on fundamental rights guaranteed under sections 34 and 35 of the 1979 Constitution which are the same rights guaranteed under sections 37 (right to private and family life) and 38 (right to freedom of thought, conscience and religion) of the 1999 Constitution. In upholding the lower court's decision, the Supreme Court held that "the right to privacy implies a right to protect one's thought, conscience or religious belief and practice from coercive and unjustified intrusion; and, one's body from unauthorized invasion."[668]

The judgment of the court in this case is important because it establishes helpful principles that will guide the lower courts in deciding cases affecting fundamental rights generally and the right to privacy in particular. Three principles can be distilled from the judgment:[669]

- The courts are the institutions society has agreed to invest with the responsibility of balancing conflicting interests in a way that would ensure the fullness of liberty without destroying the existence and stability of society itself;
- The law's role is to ensure the fullness of liberty when there is no danger to public interest;
- The sum total of the right to privacy is that an individual should be left alone to choose a course for his life, unless a clear and compelling overriding state interest justifies the contrary.

---

668 Id at 104.

669 Id at 105.

3.8 Evaluation of privacy protection in Nigeria

3.8.1 Introduction

The judicial enforcement of privacy rights in Nigeria has been minimal; the limited case law available for enforcement of privacy rights do not give much insight into how the courts regard the right to privacy. The cases discussed above dealt mainly with the aspects of privacy that concern the dignity of the human person and inviolability of the private home of a citizen or other resident of Nigeria. The statutory protections are concerned with maintaining the confidentiality of information mainly in the government's possession. Information privacy has not featured in any judicial determination to date.[670] The paucity in judicial intervention on matters concerning privacy generally, but information privacy particularly, may be attributed to three main factors outlined below.

3.8.1.1 The weak notion of privacy

Firstly, the notion of privacy is weak in the African understanding of human rights.[671] Privacy was not recognised as a human right in the *African Charter on Human and People's Rights* (ACHPR) when it was adopted in 1981. This was the case, notwithstanding the fact that two key documents of the UN namely the *Universal Declaration of Human Rights* (UDHR) and the *International Convention on Civil and Political Rights* (ICCPR) expressly guaranteed the protection of privacy at the time the African Charter was drawn up. Although many African countries adopted the human rights ideals espoused in the UDHR and the ICCPR,[672] the political leadership of these countries, including Nigeria, did not deem privacy as one of the human or people's rights that should be protected.

Although the OAU Charter, at the inception of the Organisation, made reference to

---

670 To the best knowledge of this writer; there is as yet, no decided case specifically dealing with information privacy.

671 See chp 4 par 2.5 above.

672 *Universal Declaration of Human Rights* (UDHR 1948) and *International Convention on Civil and Political Rights* (ICCPR 1966).

human rights concerns and the adoption of the principles enunciated in the UDHR and the UN Charter, the said principles seemed to be relevant only in so far as they "provide a solid foundation for peaceful and positive cooperation among states."[673] The reality in many of the then newly independent African countries and right up to the close of the twentieth century, shows that emphasis was placed more on the defence of "their sovereignty, their territorial integrity and independence."[674] Fundamental human rights were, and still are being violated.[675] According to Mahmoud, "most of the violations of human rights are often against those who speak out against the corrupt use of state resources."[676]

3.8.1.2 Limited exposure to telecommunication facilities

Secondly, and with particular reference to information privacy, a close look at the demographic and other statistical indicators of development of the Nigerian state at independence in 1960 reveals that the country had only 18 724 telephone lines for a

---

673 See a II (1) (E) OAU Charter. Oji Umozurike, a one-tine Chairman of the African Commission on Human Rights, described the prevailing attitude within the OAU thus: "The OAU maintained an indifferent attitude to the suppression of human rights in a number of independent African states by unduly emphasising the principle of non-interference..." see Umozurike 1983 (77) *AJIL* (1983) 902-903.

674 Id a II par 1 (a) and (c).

675 For example, four years after gaining independence, the government of Ghana detained more than one thousand people opposed to its policies, under the *Preventive Detention Act* of 1958. The Act permitted the President to detain persons engaged in acts considered prejudicial to state security and public order in normal and emergency times. Undeniably, the detainees' human rights were violated by the detentions. Commenting on the drastic resort to state power to protect itself for which the Nkrumah regime was severely criticised, one African scholar, Nwabueze stated that:

> The peculiar exigencies of a new state with the inherent insecurity arising from tribal or racial divisions, from the newness of the state and the immaturity and divisive politics of its leaders, and from the tensions of rapid change, justify these extraordinary measures.

See Nwabueze *Presidentialism in Commonwealth Africa* 343.

676 Mahmoud 1993 (15) *Hum Rts Q* (1993) 493. The thinking that underpins the attitude of governments in Africa to human rights and the rule of law is encapsulated in a statement attributed to the Ghanaian Interior Minister under Kwame Nkrumah when asked to justify the deportation of two critics of the government. He is reported to have boasted: "[T]here is nothing in the country of Ghana that the government cannot do, except change a man to a woman and a woman to a man."… See n 638 at 335. In Nigeria, the same thinking can be discerned in the attitude of government officials when faced with controversy arising from the government's actions or proposed actions. Eg, in the early 1990s, the National Electoral Commission adopted the open ballot voting system for then forthcoming elections. When it was pointed out that the proposed system was illegal under existing laws, a top functionary of government responded by saying, "well, it is illegal, but we can amend to accommodate it also." See Civil Liberties Organisation (CLO) *Human Rights Call: A Summary of Twelve Instances of Human Rights Violations in Nigeria between January and October 1990* 5.

population of 40 million people.[677] By 1963 when the first indigenous post-independence Constitution was enacted with provision for protection of privacy, the telecommunication infrastructure had not significantly improved. The installed telephone capacity in Nigeria in 1985 was about 200,000 lines with a tele-density equal to 1 phone to 440 inhabitants. By December 2010 however, the installed capacity in the industry stood at 157 839 million lines, while tele-density increased to 63.11% in the same period.[678] As for postal services, at the time of independence in 1960, 176 post offices, 10 sub post offices and 1000 postal agencies were in operation serving an estimated population of 40 million people.[679] With such a low exposure to communication facilities, a greater number of Nigeria's population have not had enough interaction with communication technologies and/or facilities to give them cause to seek the protection of their information privacy. Attention is still being focused on meeting demands for facilities.

The use of new technology has often in the past led to transactional conflicts, that have been litigated upon by reliance on established norms and legislation built up over a long period of time. For example, the first case in the US arising from the use of the telegraph was decided in 1856;[680] subsequently, a significant body of case law has built up over the years not only in the US, but also in many other countries regarding the use of the telegraph and the telephone. The same cannot be said however for the new information technologies such as the Internet that has only recently been introduced in Nigeria. Their usage has not yet reached such a critical mass as to elicit norms, legislations or case law relating to the conflicts arising from transactions based on the use of the new technologies.

---

677 Ministry of Communications *National Policy on Telecommunications* (2000) chp 1.

678 The Nigerian Communications Commission *Monthly Subscriber Data (September 2010 – August 2011).*

679 Current figures available from the Nigerian Postal Service show that there are presently about 955 Post Offices and over 3,000 Postal agencies throughout the Federation. According to the NIPOST, these were the figures when Nigeria's population was about 120 million people, being about 20% of the number of postal outlets it should provide to meet the Universal Postal Union's recommended ratio of 1 post office for 3000 to 6000 people. It is pertinent to note that Nigeria's population reached 167 million people in October 2011. See Nigeria Postal Services website [online]. See also the National Population Commission of Nigeria website [online].

680 *Durkee v Vermont* 29 Vt 127 (1856).

3.8.1.3 High poverty level

Thirdly, poverty in Nigeria is widespread as both income and human poverty are quite extensive. It was estimated that 66 per cent of the population or 70 million people in 2000 were classified as poor, as against 55 million people in 1998."[681] The Nigerian Bureau of Statistics, in its most recent report on the state of poverty in Nigeria in 2010, disclosed that 112.519 million Nigerians, representing about 69% of the country's population, live in poverty.[682] Thus, the high cost of the available communication facilities coupled with the high poverty level has resulted in the marginalisation of a large portion of the population. They do not, in fact cannot have access to modern communication facilities even if they wanted to.

Furthermore, the literacy level in Nigeria is low.[683] When combined with the high poverty level, the result is that many Nigerians are precluded from enjoying the benefits of modern communication. Without the opportunity to interact with modern communication technologies, many Nigerians have no reason to concern themselves with fears about the privacy of their personal information and whether it has been or is likely to be breached. Consequently, the number of persons complaining of or seeking a judicial remedy in the event of an alleged breach of information privacy is low.

This explains the paucity in the case law on the constitutional protection of privacy in general, and information privacy in particular. Even today, with the improved access to telecommunications facilities,[684] the average Nigerian user of communication facilities is still either ignorant of or indifferent to the privacy implications of the telecommunications technologies. It is arguable that even where the average Nigerian user of telecommunications and postal services is interested in enforcing his right to privacy, the laws protecting the right to privacy may not offer all the

---

681 UNDP *National Human Development Report* (2001) 43.

682 See Onuba 14th Feb 2012 *The Punch.*

683 See UNESCO Institute for Statistics *Education (all levels) profile – Nigeria* [online]. According to UNESCO, Nigeria's literacy level (% of population above 15 years able to read and write) in 2010 was 61.3%.

684 As at February 2013, Nigeria's active fixed wired/wireless lines stood at 410,664 while the digital GSM lines were over 113,399,984 lines and the CDMA lines were over 2,790,989. Total active lines in use as at February 2013 stands at 116,601,637 lines. See The Nigerian Communications Commission *Monthly Subscriber Data (September 2010 – August 2011).*

opportunities for the enforcement of the user's right.[685] It is all the more necessary therefore to adopt new laws or rather a new and comprehensive legal framework for protecting the right to privacy in the 21st century as shall be argued in chapters 7 and 8 of this thesis.

3.8.2 Other constraints on the legal protection of privacy in Nigeria

3.8.2.1 Introduction

The Constitution is the supreme law of Nigeria. Where fundamental rights are clearly enacted in the Constitution, the provisions take precedence over all other statutes or legislations on the same matters, including any rules or regulations.[686] The idea of entrenching fundamental rights in the Constitution is to strengthen their protection and prevent the government made up of the executive, legislature and judiciary, from enacting any law to weaken or outrightly remove the protections. It also prevents the judiciary from interpreting laws in any manner as to make them of no effect. Under military regimes, however, experience in Nigeria has shown that Constitutional guarantees of rights are not sacrosanct.[687] In the enforcement of the fundamental rights enumerated in Chapter 4 of the Constitution, the courts have a duty to ensure

---

685 See chp 4 par 3.5.5 above.

686 S 1(1) and 1(3) Constitution of the Federal Republic of Nigeria 1999.

687 For example, upon the collapse of the Second Republic in 1983, the then military junta promulgated the State Security (Detention of Persons) Act, Cap 414 Laws of the Federation of Nigeria 1990 (formerly Decree No. 2 of 1984), s 4 of which provides:

> (1) No suit or other legal proceedings shall be taken against any person for anything done or intended to be done in pursuance of this Act.
> (2) Chapter IV of the Constitution of the Federal Republic of Nigeria is hereby suspended for the purposes of this Act and any question whether any provision thereof has been, is being or would be contravened by anything done or proposed to be done in pursuance of this Act shall not be inquired into in any court of law and accordingly sections 219 and 259 of that Constitution shall not apply in relation to any such question.

Similarly, the Constitution (Suspension and Modification) Decree No 107 of 1993 and the *Federal Military Government (Supremacy and Enforcement of Powers Decree* No 12 of 1994, suspended the application of the human rights provisions contained in Chapter IV of the 1979 Constitution and also excluded the jurisdiction of the courts to entertain any civil proceedings that arose from anything done pursuant to the provisions of the Decrees. Case law in Nigeria is replete with judicial pronouncements to the effect that "[o]nce the provisions of a Decree or Constitution ousting the jurisdiction of the Courts on any specific matters are clear and unambiguous, the Courts are bound to observe and apply them. See *Okeke v A-G Anambra State* (1992)1 NWLR (Pt. 215) 60 at 86 per Uwaifo, JCA. See also *Lekwot v Judicial Tribunal* (1993) 2 NWLR (Pt. 276) 410 at 447, *Fawehinmi v Abacha* (1996) 9 NWLR (Pt. 475) 75.

that the rights are not whittled down or breached. The rights are subject to the exceptions and provisions clearly enacted or identified in the Constitution itself, or in existing statutes or regulations which are not in conflict with the Constitution.[688]

3.8.2.2 Constitutional derogations

The constitutional right to privacy is couched in broad terms. This is perhaps one reason why the right is not effective. Although the Constitution recognises the right to privacy, there are obvious limitations; in addition to the broad terms in which the right is couched, there is also the limitation that the right is not absolute.[689] It can be limited by any other law that has general application, in so far as the limitation is "reasonably justifiable in a democratic society" and does not conflict with the Constitution.[690] The constitutional limitations placed on the right to privacy are also couched in broad terms:

> (a) in the interest of defence, public safety, public order, public morality or public health; or
> (b) for the purpose of protecting the rights and freedoms of other persons.[691]

The fact that the limitations on the right to privacy, and indeed other rights protected

---

688 *Akulega v Benue State Civil Service Commission & Anor* (2002) 2 CHR 1.

689 Human rights are said to be absolute in the sense that they are universal and inalienable. According to Feinberg, there are three possible interpretations of the term "absolute"; the first interpretation could mean that all rights are "unconditionally incumbent within the limits of their well-defined scope". The second interpretation suggests that they are "ideal directives" and all the parties involved in the implementation of human rights should "do their best" to implement the rights in all circumstances. For example, if the state has taken a piece of land from "A" or "B", the state should compensate him since he has a right to his property. The third interpretation of the absoluteness is also the strongest, that is, human rights should be honoured without exception. The right to free speech would be absolute in the sense that it is protected in all circumstances. In this sense, the limits of the right would be in consonance with the limit of what is specified permissible conduct and no infringement of the right in any form would be permitted. See Feinberg *Social Philosophy* 85.

690 S 45(1) of the Constitution provides that:
Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society-
(a) in the interest of defence, public safety, public order, public morality or public health; or
(b) for the purpose of protecting the rights and freedoms of other persons.

691 Ibid.

in the Bill of Rights (Chapter IV of the Constitution), are stated in broad terms, has often given the various governments in the federation (Federal, state and local) the impetus to derogate from the constitutional provisions. Under the above terms, interference by the state with the privacy rights of individuals will readily be excused as being in pursuit of one of the objectives outlined in the limitation clause. Thus, infringements of private communications through interception and surveillance would be regarded as reasonable if authorised by a judge or other authority,[692] where a serious offence is concerned, or where the security of the country is at risk. Similarly, searches and seizures without a warrant which would ordinarily be an unconstitutional violation of the privacy right are allowed in the *Criminal Procedure Act*.[693] The problem, however, is that many of the derogations are without regard to due process and often in pursuit of political opponents and critics under the ambiguous cover of "national security".[694]

3.8.2.3 A deficient culture of respect for the rule of law

Privacy is a fundamental human right just like other rights such as freedom of expression and freedom of movement. One of the functions of privacy, according to Westin, is to protect the individual from improper surveillance and shield those institutions, such as the press, which operate to keep the government accountable.[695] Privacy is protected in many countries of the world and is the subject of a number of

---

692 Eg, s 19 of the Nigeria Postal Service Act, Laws of the Federation of Nigeria 2004, provides that:

> On the occurrence of public emergency or in the interest of public safety or tranquillity, the Minister may by order in writing direct that a postal article or or class or description of postal articles be intercepted or detained or be delivered to an officer of the government mentioned in the order or be disposed of in such manner as the Minister may direct.

693 S 6(1) Criminal Procedure Act, Laws of the Federation of Nigeria 1990 makes provision for the searching of arrested person by arresting officer where bail has not been granted, while s 7(1) allows an arresting officer having reason to believe that the person to be arrested has entered into a premises to escape arrest, to forcibly enter into the premises to search for and arrest the person.

694 Several Human Rights Reports by the US Department of State on Nigeria, highlight recurring instances of arbitrary interference with privacy, family, home and correspondence, by the Nigerian Police and other security agents of government by way of raids on homes without warrants, placing relatives and friends of wanted suspects in detention without criminal charge to induce suspects to surrender to arrest; and surveillance and interception of communications of members of the opposition or civil rights groups. See for example US Department of State *2010 Human Rights Report: Nigeria* [online].

695 Westin *Privacy and Freedom* 25.

international covenants and human rights treaties.[696] In Germany for example, the Federal Constitutional Court recognised that state storage of personal data, especially in computer systems, could influence the citizen's behaviour and endanger their general liberty of action and must therefore be considered as a violation of civil liberties, thus recognizing the citizen's "right of informational self-determination."[697]

This is, however, not quite the case in Nigeria; although the Nigerian Constitution protects the privacy of its citizens,[698] as with many of the other fundamental rights, the observance is more in the breach than its protection. For example, a newspaper report in 2006 informed its readers that a combined team of Nigerian security officials "... stormed the Tafawa Balewa Headquarters of the then Platinum Habib Bank in Lagos where they forcefully obtained the banking records of Vice President Atiku Abubakar."[699] According to the report, the raid on the bank occurred after the Vice President raised alarm that the government was making efforts to dig up incriminating evidence against him to forestall his presidential ambition.[700] The tenor of the report suggests that the financial records of the Vice President were obtained without due process and certainly without his consent or that of the bank. It seems that in the face of an allegation of corruption, recourse to privacy rights is excluded.

The apparent absence of due process and obvious breach of the banker/customer confidentiality that exists between the bank and the Vice President is a pointer to how privacy (and indeed other rights) is regarded in the country.[701] It is of course

---

696 Art 12 *Universal Declaration of Human Rights* 1948; Art 17 *International Covenant on Civil and Political Rights*, 1966; Art 8 *European Convention for the Protection of Human Rights and Fundamental Freedoms*, 1950.

697 65 *BVerfGE* (Decisions of the Federal Constitutional Court) 1 42 (1983); referred to in Hornung and Schnabel 2009 (25) *CLS Rev* 84.

698 S 37.

699 Lohor, Akunna, and Andoor 13th July 2006 *Thisday*.

700 There are immediate and remote reasons that may account for the action of the security agents; one reason may be the perception, and indeed, allegations of corruption that pervades Nigeria's political class of which the Vice President is a very visible member. Most Nigerians will however agree that one of the immediate reasons for the raid is the fact that the Vice President stood resolutely against plans by lobbyists for a third term for the incumbent President, contrary to the two terms provided for by the Constitution.

701 Public policy in Nigeria acknowledges the Constitutional right to privacy; for example, a Central Bank of Nigeria guideline on e-banking reiterates the need for banks to protect the privacy of customer's data by

arguable that where the legislature has made a law allowing for the derogation of the right in the light of exceptions allowed by the Constitution, reliance on the provision of that law would be justified. This would indeed be the argument of the Economic and Financial Crimes Commission (EFCC) that carried out the raid, that the legislation establishing the EFCC contains such derogation and therefore their actions are protected by the law.

The government's interest in having access to relevant financial transaction data in order to combat terrorism, detect crime and punish offenders cannot be denied. However, short-term decisions to permit the breach of due process and privacy rights without giving due consideration to the long-term negative effects of such breaches, undermines the rights of the citizens and ultimately subverts the democratic process and the rule of law. This is more so the case in Nigeria where there is no history of ensuring good governance and where judicial oversight and/or intervention is often deliberately excluded or perverted by state power, particularly under military regimes.

3.8.3 Conclusion

The cases on privacy discussed above dealt mainly with privacy issues relating to the dignity of the human person and inviolability of the private home of a citizen or other resident of Nigeria. Information privacy is yet to receive judicial pronouncement in Nigeria. There are two reasons why the Nigerian judiciary needs to acquaint itself with the emerging jurisprudence of information privacy law in other jurisdictions. The first reason is that Nigerians are increasingly using new information technology tools in their homes, offices and businesses. Inevitably, transactional conflicts will arise as more people use these technologies; they will look to the courts for help in resolving the conflicts. The courts and the practitioners engaged in the justice system

---

ensuring that:

- Customer's personal data are used for the purpose for which they are compiled.
- Consent of the customer must be sought before the data is used.
- Data user may request, free of cost for blocking or rectification of inaccurate data or enforce remedy against breach of confidentiality.
- Processing of children's data must have the consent of the parents and there must be verification via regular mail.
- Strict criminal and pecuniary sanctions are imposed in the event of default.

See Central Bank of Nigeria *Guidelines on Electronic Banking* [online].

must be familiar with current trends in technology usage and the implications they have on the rights of the people. Only then can the system effectively administer justice in the face of rapid technological progress.

Also, more Nigerians will become aware of the pervasive and automated collection of their personal information by both government and private entities and will eventually demand greater protection by way of legislation to prevent abuse. It is certain that the mere aggregation of rules and regulations without a knowledgeable judiciary versed in the demands and challenges of the digital environment will not be enough to secure the citizens privacy rights. There is need therefore, for Nigerian lawyers and judges to acquaint themselves with current trends in other jurisdictions with regard to the protection of information privacy and how problems associated with impact of technology on rights of the citizen are dealt with. This will be helpful in dealing with domestic conflicts in the digital environment.

The second reason is the European Union's compulsory regulatory regime for the protection of personal information of European citizens.[702] The EU *Directive 95/46/EC* is one of the contemporary global norms that Nigeria's judicial, trade and business policies need to be consistent with. One area where this is inevitable is in regard to communication data which has assumed an unprecedented importance in international economic activities in the last two decades. This is principally because industries such as banking, insurance, airlines, multinational trading companies and news companies depend largely on instant access to information which they in turn redistribute across the world.[703]

The flow of data across national boundaries, generally referred to as trans-border data flow, continues to expand as more countries and multinational companies engage in the lucrative trade in information goods and services. Concerns about the privacy of individuals with regard to the collection, storage and use of personal information about them prompted various countries to adopt data protection measures by way of legislations to protect information privacy. The significance of

---

[702] *Directive 95/46/EC.*

[703] Mowlana *Global Information and World Communication* 107.

the legislations adopted by members of the EU under the above Directive is the demand it makes on third party nations to provide an adequate level of information privacy protection in their regulatory regimes to safeguard the privacy of collected data about Europeans. Nigerian lawyers and judges need to see that trans-border data flows arising from the globalisation of national economies and aided by the increasing trade in information goods and services, are commodity flows that have acquired economic significance and need to be protected. The movement of data across borders confronts governments with:

> [T]he tension between the conflicting state interests in protecting, conserving, and controlling information on the one hand, and of importing, exporting, and exchanging ideas on the other – both in pursuit of state goals and in support of national policies.[704]

To balance the competing interests of promoting and restricting the flow of personal information, a knowledgeable judiciary that is well acquainted with contemporary issues in an information-dependent world is required. A key issue the courts will have to deal with will be the protection of information privacy. Nigerian courts must therefore be ready to enforce information privacy/data protection. As one commentator has observed, as long as the EU remains firm on the *Directive*, the European market remains important enough to compel global privacy regimes to match the Union's requirements.[705] The US was persuaded[706] to respond positively to the EU *Directive* by adopting the "Safe Habor" principles.[707]

---

704 Gotlieb, Dalfen and Katz 1974 (68) *AJIL* 227.

705 Loukidelis *Transborder Data Flows and Privacy* [online].

706 It is said that "[t]he EU and the US economies account together for about half the entire world GDP and for nearly a third of world trade flows." See European Commission *Trade* [online]. With such a commanding grip on world trade, it is understandable why access to each other's markets is of such great importance to both the US and the EU. This importance persuaded both parties to agree on the Safe Harbor principles for the protection of personal information privacy that would enable the transfer of personal data from the EU to the US.

707 The "Safe Harbor Principles" constitute a framework agreement between the US and the EU to provide for the transfers of personal data from the EU to US companies and other establishments that adhere to a set of principles issued by the US Department of Commerce. Under this arrangement, US companies would annually self-certify that they met the agreed set of seven privacy principles on data protection issued by the U.S. Department of Commerce. Also, the US Federal Trade Commission (FTC) would maintain a list of complying organisations on its website; failure to comply would be actionable under the Federal Trade Commission Act. The EU recognises the principles as providing "adequate protection" as required by the EU *Directive* (a 25(6)). The agreement was signed in the year 2000. See Export.gov website [online].

However, the problem is not entirely that of the court and its practitioners. As the judges themselves have noted, if there are statutes in place recognising a right and then prescribing derogations from such rights, the courts will have no other recourse than to apply them. As I have shown earlier, it is obvious that the constitutional and statutory provisions for the protection of the right to privacy are inadequate to allow for a more robust enforcement of the right. There is an urgent need to reform Nigerian laws in general but particularly those laws that regulate interactions and activities in the digital medium and facilitated by ever innovating ICTs. This is all the more necessary when it is evident that the laws presently protecting privacy were made in an era when ICTs were not common features of the Nigerian society. The Nigerian Law Reform Commission and the National Assembly must work in cooperation with all other stakeholders in the judicial and economic sectors of the country to amend or make new laws to address the realities that the information revolution have thrown up in Nigeria in recent times. Law reform notwithstanding, Nigeria still needs an activist judiciary that can make inroads in this area of the law and give effect to the new and amended laws when they do get enacted.

Finally, the fact that Nigeria accounts for a negligible percentage of world trade despite her acknowledged potentials, prompted the government to formulate a new Trade Policy.[708] The Policy seeks among other things, to make Nigeria a full partner of the global economy. It recognizes that:

> For Nigeria to succeed in the emerging global market, we must move away from the traditional practices, which are fast becoming obsolete and face the new challenges. Above all, our business policy must be seen to be transparent, stable and consistent with contemporary global norms.[709]

If the objectives outlined in the national Trade Policy and other policy documents[710] are to be realised, there is no question that Nigeria must respond to the EU *Directive*

---

[708] Federal Ministry of Commerce *Trade Policy of Nigeria* (2001). In 2011, the government of Nigeria commenced the review of the National Trade Policy. In announcing the review, the Minister of Trade and Investment noted that the review became necessary because the current trade rules, regulations and practices outlined in the current Trade Policy are outdated. The new Trade Policy is expected to be ready in June 2013. See Williams 22 February 2013 *Dailytrust*.

[709] Ibid at p 1.

[710] NITDA *National Policy for Information Technology* [online].

on data protection. From an economic and business perspective, businesses in many parts of the world are realising that:

> As awareness of privacy builds, any company that doesn't treat privacy as a core business issue will find itself at a disadvantage in the Internet marketplace. Its customers will have more reason to abandon their loyalties and will be less likely to buy its products... Ignoring privacy reflects negatively on a company's brand, which, in a society of networked consumers who are increasingly savvy about privacy issues, can fall out of favour literally overnight.[711]

The same arguments can be made for the Nigerian state and its business sector. In chapters 7 and 8, the question whether Nigeria should respond to the EU *Directive* on data protection and what such a response should be will be more fully examined. It suffices for now to say that from a judicial, business and economic perspective, there is a need to uphold privacy and the freedom of information, notwithstanding their underlying tensions. In the next chapter, the underlying tensions between privacy and freedom of information will be discussed.

[711] Cavoukian and Hamilton *The Privacy Payoff: How Successful Businesses Build Customer Trust* 92.

CHAPTER 5

HOW UNREGULATED ACCESS TO INFORMATION INTERFERES WITH INFORMATION PRIVACY: RECONCILING PRIVACY WITH FREEDOM OF INFORMATION

1. AIM OF CHAPTER

The purpose of this chapter is to explore how unbridled access to information and the global trade in information and information products affect information privacy. It traces the historical development of the use of technology in the collection of information and the commercial uses of personal information. The increased collection of information was in part greatly spurred by the realisation that information collected, when processed and aggregated, could be sold for profit. The chapter highlights the business models that utilise personal information in the new marketplace where information and information products are sold. Information is a global resource with unlimited potential for all and today, most national economies place a high priority on the efficient management of information.

I will argue firstly, that even though information is so readily available thanks to modern technologies that allow the collection, processing and storage of information, in many parts of the world, information is not so readily accessible. Governments around the world, and increasingly so, small segments of the private sector, have become enormous storehouses of information. A significant portion of the information kept by governments is collected with the help of taxpayers' money, and yet the public do not have free and ready access to the information. There is therefore a poverty of information caused mainly by the fact that many governments, particularly in developing countries, deliberately withhold much of the information from the public. Another reason is the lack of appropriate technologies with which to access needed information. Thus, there is on the one hand, increasing availability of

information aided by computer technology and on the other hand, a struggle for access to such information. The struggle for access to information has yielded various Freedom of Information laws in many countries, which have widened access to information, including personal information. While this widened and legally-backed access to government-held information will enhance transparency, accountability and good governance, it will also engender new threats to information privacy.

Prior to the widespread use of ICTs, only very little information was stored because of the lack of storage facilities and the very high costs of storing information in an easily retrievable form. There was therefore very little incentive and opportunity to misuse stored information. This state of affairs in effect deterred unauthorised disclosure of personal information and thus helped to protect the privacy of personal information. This is no longer the case because advances in computer technology continuously expand the scope and capacity for collecting, processing, storing and disseminating information. Furthermore, the realisation that information, as a commodity, can yield great profits for those who harvest and sell the new commodity has provided great incentive to exploit this "new" resource and ensure that the free flow of information is unimpeded. This unbridled flow of information has generated great concern for the protection of personal information privacy in particular, and privacy generally.

The long-standing conflict between the right to privacy and right to information are highlighted in this chapter. The conflict is highlighted because both the right to freedom of information and the right to privacy are fundamental human rights and one does not have any primacy over the other. Moreover, technological advances in the collection of information and the new business models for trading in such collected information seriously threaten the whole notion of information privacy.

1.1. INTRODUCTION: ACCESS TO INFORMATION

At the inception of the United Nations Organisation in 1946, the General Assembly of the new organisation resolved that "[f]reedom of information is a fundamental human right and the touchstone for all freedoms to which the United Nations is

consecrated."[712] The right to seek and receive information is thus not simply a converse of the right to freedom of expression which is guaranteed in many constitutions, but a right on its own. When people are denied information, they are denied the opportunities to develop to their fullest potentials; they are also denied access to the fullest range of their fundamental human rights. The personality, political and social identity and economic capability of people are determined to a large extent, by the information available to them.[713] The right of access to information would encourage the full participation of citizens in the democratic process by empowering them to get relevant information that would enable them to make informed choices.

The right of access to information is at the core of the whole gamut of human rights enjoyable by persons in different countries. It is information, or rather, access to information, that enables citizens of a country to exercise their rights, determine when those rights are at risk or have been breached, and know who is responsible for the breach.

1.1.1 The fundamental right to freedom of information

The right to information as a fundamental right is usually expressed in terms of freedom of information. The freedom to seek information is guaranteed by international law[714] and is most commonly understood as a right to access information held by public bodies on request.[715] While this constitutes the core element of the right, it also encompasses, as some have argued, an obligation on the government and public agencies to make information about their activities available and accessible to the public.[716] What then, constitutes the individual's right to

712 United Nations General Assembly Resolution 59(1).

713 Commonwealth Human Rights Initiative Report *Looking for the Right to Information in the Commonwealth* 12.

714 Art 19 *International Covenant on Civil and Political Rights* (ICCPR); other international instruments are the *European Convention on Human Rights and Fundamental Freedoms* (European Convention, Art 10), the *African Charter on Human and Peoples Rights* (ACHPR (1981), Art 9) and the *Inter-American Convention on Human Rights* (ACHR (1969), Art 13).

715 Mendel *Freedom of Information: A Comparative Legal Survey* v [online].

716 Ibid. According to Mendel, this element of obligation to publish information is to be found in many of the freedom of information laws around the world today.

information and the government's obligation to provide information?

1.1.2 The individual's right to access information

In his article "Freedom of Expression", Joshua Cohen[717] identified three fundamental interests that are protected by a right to information. The three fundamental interests are: (1) the interest in expression, (2) the interest in deliberation and (3) the interest in knowledge.[718] According to Cohen, the interest in expression is "a direct interest in articulating thoughts, attitudes, and feelings on matters of personal or broader human concern and perhaps through that articulation influencing the thought and conduct of others."[719] Thus, access to information creates the enabling environment for the writer to express himself by connecting with the reader of the information accessed.

Also, for acts of expression to be possible and meaningful, people need a rich pool of information that will allow them to develop their ideas and learn how to communicate them effectively. Access to information enables an individual member of a society not only to express himself but also to receive the expressions of other members of his society.[720]

Secondly, the individual's access to the expressions of others as well as his own ability to express himself, enables the individual to satisfy what Cohen refers to as "deliberative interests." The interest in deliberation speaks of the individual's ability to revise and gain a deeper understanding of his individuality and the collectively held beliefs and commitments of the community.[721]

The third interest, the interest in knowledge, allows the individual to aggregate and leverage the totality of the information he has accessed in order to satisfy his "informational interests" which constitute the individual's "fundamental interest in

717 Cohen 1993 (22) *Phil & Pub Aff* 207.

718 Ibid at 223-230.

719 Id at 224.

720 See a 27 *of* the *Universal Declaration of Human Rights.*

721 See n 717 at 229.

securing reliable information about the conditions required for pursuing one's aims and aspirations."[722] Without access to such knowledge, individuals and groups will be unable to effectively carry out their aims. In order for the citizens of any given society to be able to exercise their rights meaningfully, they must be given access to information. If they are not aware of the fact that they have rights or what the rights are, then it is difficult to see how they can meaningfully enjoy their rights. For example, in the Canadian case of *Jane Doe v. Board of Commissioners of Police for the Municipality of Metropolitan Toronto et al,*[723] the court recognised that the right to security creates a corollary right to information about threats to personal safety which would be violated if the police force knew of a threat and failed to provide that information to the threatened individual.[724]

Without access to information therefore, the individual's interest in knowledge and his capacity to leverage that knowledge cannot be realised. When members of a given society have access to information held by the government and its agencies and bodies, the access to information is what protects them against abuses, corruption, mismanagement and disenfranchisement by the government. Increasingly, governments around the world are realising that giving the citizens access to government-held information can also be beneficial to governments themselves. However, much of the debate on access to information centres on whether governments are obligated, by the international and national enactments on access to information, to provide information and the extent of such obligation if any.

---

722 Ibid.

723 See Ontario Court (General Division), Court File No 87-CQ-21670, Judgment July 3, 1998.

724 In order for the citizens of any given society to be able to exercise their rights meaningfully, they must be given access to information. If they are not aware of the fact that they have rights or what the rights are, then it is difficult to see how they can meaningfully enjoy their rights. The court in the *Jane Doe v. Board of Commissioners of Police for the Municipality of Metropolitan Toronto et al*, case recognised that the right to security creates a corollary right to information about threats to personal safety which would be violated if the police force knew of a threat and failed to provide that information to the threatened individual.

1.1.3 Is there an obligation on government to provide information?

The question whether the government is obligated to provide information is a long-standing one. Activists and NGOs have argued that states are under a substantive positive obligation to ensure that citizens have access to information about human rights violations.[725] Others, however, do not see such an obligation. Referring to the *International Covenant on Civil and Political Rights* (*ICCPR*), Sir Anthony Mason[726] argued that the provisions of article 19 paragraph 2 thereof impose no obligation on governments or government agencies to disclose information not already in the public domain. According to him, "[t]he paragraph does not expressly impose an obligation to provide information or a right to obtain it."[727] He concedes, however, that there remains the possibility that paragraph 2 may be interpreted at some point to recognise an obligation on state agencies to make available information which is not already available. According to him, the fact that freedom of expression and information are so essential to modern democratic governance will dictate such recognition.[728]

In a similar vein, article 10 of the *European Convention on Human Rights and Fundamental Freedoms* (ECHR),[729] guarantees the freedom to hold opinions and to receive and impart information and ideas. The debate whether the right to information imposes an obligation on the state to make information available of its own motion, is reflected in the case law of the European Court of Human Rights (ECtHR) in its interpretation of article 10 of the ECHR. While acknowledging "the right of the public to be properly informed"[730] and "the public's right to be informed of a different perspective"[731], the Court stopped short of accepting a duty on public

---

725 See n 715.

726 Mason "The Relationship Between Freedom of Expression and Freedom of Information" 227.

727 Ibid.

728 Ibid.

729 Council of Europe *European Convention on Human Rights (as amended by Protocols Nos. 11 and 14) (CETS 5).* (4th November 1950*).*

730 ECtHR 26 April 1979, *Sunday Times (no 1) v United Kingdom*, §§ 64-66. See also ECtHR 8 July 1986, *Lingens v Austria*, § 41; ECtHR 25 June 1992, *Thorgeir Thorgeirson v Iceland*, § 63.

731 ECtHR 18 July 2000; *Sener v Turkey* § 46.

authorities to actively provide information to the public.

In its judgment in the case of *Sirbu and others v Moldova,*[732] the European Court of Human Rights, referring to its earlier case-law, reiterated that:

> [F]reedom to receive information … cannot be construed as imposing on a State, in circumstances such as those of the present case, positive obligations to disclose to the public any secret documents or information concerning its military, intelligence service or police.

In his report[733] to the UN Commission on Human Rights in 1995, the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression was of the view that "the right to seek, receive and impart information imposes a positive obligation on states to ensure access to information, particularly with regard to information held by government in all types of storage and retrieval systems including film, microfiche, electronic capacities and photocopies."[734]

Notwithstanding the Special Rapporteur's reports affirming the positive obligation on the state to provide information to its citizens, a judicial validation of his position has not been unanimous.[735] For example, the ECtHR, for much of its history, refused

---

[732] ECtHR 16 June 2004 § 18. In using the phrase "circumstances such as the present case" in its judgment, the European Court of Human Rights gives an impression that in different circumstances, a different decision upholding a positive obligation might result. Nevertheless, since the decision in the Sirbu case was given, it seems that no case before the Court presented any different set of circumstances to enable the Court see it's way clear to declaring a positive obligation on the State to provide information in its custody.

[733] Hussain A *Report of the UN Special Rapporteur on Promotion and Protection of the Right to Freedom of Opinion and Expression* (1998) par 14.

[734] Ibid. In his Report for 2000, the Special Rapporteur reiterated that:

> … the right to seek, receive and impart information is not merely a corollary of freedom of opinion and expression; it is a right in and of itself. As such, it is one of the rights upon which free and democratic societies depend. It is also a right that gives meaning to the right to participate which has been acknowledged as fundamental to, for example, the realization of the right to development. See Hussain *Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (2000) 15.

[735] See the decisions of the European Court of Human Rights in the following cases: *Leander v Sweden* (1987) 9 EHRR 433; *Roche v United Kingdom* (2006) 42 EHRR 30 (all holding that there is no obligation on the state to provide information); see the American case of *Houchins v KQED, Inc*. 438 US 1 at 16 (1978); in contrast however, see the decisions in the following cases: *Claude-Reyes et al v Chile* (2006) (The Inter-American Court of Human Rights held "… that by expressly stipulating the right to "seek" and "receive" "information," Article 13 of the Convention protects the right of all individuals to request access to State-held information, with the exceptions permitted by the restrictions established in the Convention.

to recognise a general right of access to state-held information. The Court may have been concerned about the implications of reading a general right to access information held by public authorities into Article 10 of the ECHR.[736]

However, in the recent case of *Gillberg v Sweden,*[737] the ECtHR upheld the right of two researchers to access research data held by a public university. According to The Open Society Justice Initiative[738] this is the first time that the Grand Chamber of the Court has recognized a self-standing right of access to information held by public authorities. The decision in the Swedish case suggests the possibility of a change in the jurisprudence of the ECtHR which had been built upon the premise that there is no violation of the right of access to official information under Article 10 when a governmental body withholds such information.[739] The decision in the *Gillberg* case accords more with the position taken by the Special Rapporteur and other international organisations and NGOs such as the UN, the Commonwealth, Organisation of American States (OAS) and Article 19.[740]

The brief review of international case law on the right to information particularly with regard to state obligation to provide information indicates a growing consensus of opinion that states have a positive obligation to provide the information they hold to their citizens. This should never have been in doubt given the fact that the disclosure of information collected by the State plays such an important role in a democratic society by enabling the citizens to meaningfully debate the activities of the government and hold it accountable. The obligation on State parties to provide

---

Consequently, this article protects the right of the individual to receive such information and the positive obligation of the State to provide it, so that the individual may have access to such information …" (at 41)); *S. P. Gupta v President of India and Others* (1982) AIR (SC) 149 (referred to in Mendel *Freedom of Information as an Internationally Protected Human Right* (2003) 3 n 11.) (the Indian Supreme Court stated that "The … disclosure of information in regard to the functioning of government must be the rule and secrecy an exception justified only where the strictest requirement of public interest so demands").

736 Mendel 2003 (1) *CMLJ* 2.

737 (2010) ECHR 1676.

738 See the case review by Pavli *Is Europe's Top Court Finally Embracing Right to Know?* [online].

739 See for example, *Leander v Sweden* (1987) 12 EHRR 433; *Roche v United Kingdom* (2006) 42 EHRR 30.

740 For a fuller discussion of the trends in the development of the right to information, see Mendel *Freedom of Information: A Comparative Legal Survey* [online]; Banisar 2010 (16) *EAJP&HR*.

information is all the more necessary now because, as Mark Bovens argues, with the decline of the industrial era and the rise of the "Information Society", the world needs to update its constitutional frameworks to take into account the new universal right to information.[741]

1.2 Freedom of Information laws

In countries where the right to information is fully realised, access to information is made possible and guaranteed by freedom of information laws.[742] Such laws provide a legally enforceable right to access official documents. In some countries, the right is further enhanced by the establishment of a specialised independent agency to regulate and enforce the freedom of information legislation.

Freedom of information laws generally seek to balance competing values and interests between the public's right to know, the individual's right to privacy and the government/public institution's mandate to serve "the public interest." A freedom of information law seeks to create an open society in which the government can be truly accountable to the people. Because democracy thrives in an atmosphere of accountability and good governance, the public have a right to scrutinise the actions of their leaders and to engage in full and open debate about their actions.[743]

Over the last century, many developed countries have adopted freedom of information policies and laws;[744] newly democratic countries are also adopting policies that encourage access to information by recognising the right to information in their Constitutions. For example, the South African Constitution of 1996[745] not only guarantees the right to access information held by the State, but also to

---

741 Bovens 2002 (10) *JPP* 317. See also Roberts 2001 (51) *UTLJ* 262.

742 See Right2info *Access to information laws: overview and statutory goals* [online]. Eg, in Africa, nine countries, namely Angola, Ethiopia, Guinea Conakry, Liberia, Nigeria, Rwanda, South Africa, Uganda, and Zimbabwe, have access to information laws (see Right2info *List of Countries with Actionable ATI Laws* [online]).

743 See n 713.

744 According to right2Info.org, a web portal with up to date information on freedom of information laws and movements around the world, as of September 2012, there were about 93 countries with right to information laws worldwide. See Right2INFO.org website [online].

745 Art 32Constitution of the RSA, 1996.

information held by private bodies. The Constitution required the government to pass a law giving effect to this right within three years of its coming into force.[746] In compliance with this requirement, the enabling legislation, the Promotion of Access to Information Act,[747] came into force in March 2001.

Freedom of information laws create a tension between the public's right to know and be informed on the one hand, and the desire of the state and its agencies to reveal as little as possible of the details of its operations. Openness is essential for the proper functioning of government as it increases the citizens' knowledge of the ways of government and thereby, increases respect for the law and promotes strong confidence in judicial remedies. This would not be possible in a system characterised by secrecy. As noted by the former Chief Justice of the US, Justice Warren Burger, "… [t]o work effectively, it is important that society's criminal process 'satisfy the appearance of justice,' … and the appearance of justice can best be provided by allowing people to observe it."[748] Because public trust in governments and governance generally has eroded considerably in recent years, many governments across the world have had to accommodate freedom of information laws and institutionalise freedom of information regimes.

An ideal Freedom of Information law should therefore give the citizens, other residents and indeed all interested parties, the right to access information held by the government without the pre-condition of establishing the individuals' interest in the information sought or legal standing to make a demand.[749]

---

[746] Art 32(2) and Sch 6, item 23 of the *Constitution of the RSA, 1996*.

[747] Act No 2 of 2000.

[748] *Richmond Newspapers Inc v Virginia* 448 US 555 at 571-572 (1980).

[749] Ackerman and Sandoval-Ballesteros 2006 (58) *ALR* 93.

1.3 Right to freedom of information in Nigeria

1.3.1 Introduction: The culture of secrecy

Prior to June 2011, a right of broad access to information held by the government in Nigeria was never acknowledged by the various governments, nor clearly articulated by the legislature and judiciary. This absence of a concept of freedom of information conforms to the ethos of secrecy that has been the hallmark of the Westminster style of government which the British colonial administration entrenched in the Nigerian civil service. This ethos of secrecy took the view that all official information is secret unless government chooses to disclose it.[750]

The Westminster style of government that was left behind by the British did not allow for openness and transparency; the government tightly controlled and to a large extent, still controls information and determines if, when and how information is released to the public. In the absence of a general right of access to information, either under the common law, the Constitution or statute, sweeping assertions of executive prerogative of secrecy permeated every facet of governance in Nigeria to the present day. This culture of secrecy is legitimised by a number of legislations, the most prominent of which is the Official Secrets Act.[751]

Under these laws, a number of terminologies such as "Secret", "Top Secret", "Confidential", "Strictly Private and Confidential" and "Classified" are used to deny the citizenry access to information. These secrecy laws enjoy blanket application and cover virtually all documents and records that originate from the government. The atmosphere of secrecy engendered by the secrecy laws is inimical to a democratic dispensation for, "informed public opinion is the most potent of all restraints upon misgovernment."[752] The return of Nigeria to civil rule in 1999 and the various efforts by the citizenry and the political class to establish democracy appears not to have

---

750 Palmer "Freedom of Information: The New Proposals" 250.

751 Cap 335 Laws of the Federation of Nigeria 1990. See also s 97 (1) of the Criminal Code Act Cap 77 Laws of the Federation of Nigeria 1990. The Official Secrets Act, as amended by the Criminal Procedure (Amendment) Act of 1966 makes it an offence for any person to transmit any classified matter to any person to whom he is not authorised by the government to reproduce or retain.

752 *Grosjean v American Press Co* 297 US 233 240 (1936).

made a significant impact on the culture of secrecy that pervades the governance.

The struggle for human rights and democracy in Nigeria was constrained for many years by the lack of information. Civil society groups, non-governmental organisations (NGOs), human rights activists, labour unions and all other special interest groups who require information for their advocacy, mobilisation and other activities, are frequently denied access to the information essential for their activities.[753]

---

[753] In Nigeria, restriction of access to information usually manifests in the following ways:

- The deliberate classification or reclassification of information no matter how insignificant, as secret, top secret, confidential or restricted. This arises from the ingrained habit of the public servant to hoard information as a power component.
- The subjection of government officials to a long-term or even everlasting duty of confidentiality even when the need for such confidentiality has lapsed.
- The routine denial of access to official or independent sources of information.

See Ekpu *FOIA: Freedom For All* 11. Two examples of how the above restrictions operate are given below:

In October 2003 during the Obasanjo administration, the *Punch* newspaper wrote to the Secretary to the Federal Government of Nigeria requesting for a copy of the Okigbo Panel Report which probed the management of $12billion oil windfall from the 1991 Gulf War. In response to the demand and reminders by *Punch* for the report, the Federal Government, in a reply to *Punch* letters of October 13 and 27, 2003 to the Secretary to the Government of the Federation, Chief Ufot Ekaette, gave an indication that efforts were being made to retrieve the Report. After waiting endlessly for the Report and not receiving any, the newspaper noted in an editorial that:

> Not a few Nigerians implicated by these probes still walk tall in the streets as free men, while some of them are holding or eyeing sensitive public offices. The non-availability of a document of such profound importance as the Okigbo Panel report is a tell-tale clue on the contempt with which officialdom holds the anti-corruption campaign. It is tragic that probes in the country scarcely lead to punishment for culprits or the furtherance of justice and transparency in public life. The fate of past probes and the reports therefrom confirm the painful fact that inquiries have become tools used to divert public attention from official corruption, ineptitude and other crimes, or to intimidate and blackmail political opponents.

See *Punch* Editorial 18 November 2003 [online]; see also Obe *The Challenging Case of Nigeria* 143 at 156.

Similarly, a Nigerian NGO, Media Rights Agenda (MRA) wrote to the Code of Conduct Bureau pointing out that the newly inaugurated President Obasanjo ought not to have been sworn in as President until he had filed his assets declaration. Receiving the reply of the Bureau that the President had indeed declared his assets before a Commissioner for Oaths, the organisation requested a copy of the declaration. The Bureau responded that there was no law requiring the President to make a public declaration of his assets, unless the National Assembly were to prescribe such. Following the Bureau's refusal to avail the MRA of the assets declarations, it filed a suit at the Federal High Court asking it to compel the Bureau to release the asset declarations to it. The court struck out the suit on the grounds that the National Assembly had not prescribed the terms and conditions for citizens to exercise such right. See MRA *Code of Conduct Bureau Declines to Release Assets Declarations by Public Officers* [online].

1.4 The campaign for access to information in Nigeria

Nigeria is a party to a number of international instruments that seek to guarantee and protect access to information. These instruments include the *Universal Declaration of Human Rights*[754], the *International Covenant on Civil and Political Rights*[755] and the *African Charter on Human and People's Rights*[756]. Furthermore, the African Union's *Declaration of Principles of Freedom of Expression in Africa,*[757] drawn up by the African Commission on Human and People's Rights in 2002 in Banjul, also forms part of the body of international instruments that apply to Nigeria by virtue of its membership in the organisation. These instruments impose a duty upon Nigeria to guarantee and protect the right of access of the citizens to information held by the government.

Furthermore, Nigeria is a member of the Commonwealth. In 1999, the Commonwealth Heads of Government adopted The *Principles and Guidelines on the Right to Know*[758] at the summit held in Durban, South Africa. The principles and guidelines adopted recognise that access to relevant information by the people empowers them to make informed choices and better exercise their democratic rights. It enhances the accountability of government, improves decision - making, provides better information to elected representatives, enhances government credibility with its citizens and provides a powerful aid in the fight against corruption.[759] This can only be achieved by guaranteeing a legal and enforceable right of public access to official information.

---

754 UN *The Universal Declaration of Human Rights* (1948).

755 UN *International Covenant on Civil and Political Rights.*

756 African Commission on Human and People's Rights *The African Charter on Human and People's Rights* (OAU Doc. CAB/LEG/67/3 rev.5; 1982 (21) ILM 58) (1981). The provisions of this Charter have been incorporated into Nigeria's domestic law under the African Charter (Ratification and Enforcement) Act, Cap 10 Laws of the Federation of Nigeria 1990.

757 African Commission on Human and People's Rights *Declaration of Principles of Freedom of Expression in Africa.* The Declaration of Principles on Freedom of Expression in Africa was adopted by the ACHPR at its 32nd Ordinary Session held in October 2002. In 2012, the Commission adopted a resolution to modify the Declaration of Principles on Freedom of Expression to include Access to Information and Request for a Commemorative Day on Freedom of Information.

758 Commonwealth Heads of Government *Principles and Guidelines on the Right to Know.*

759 Ibid.

In 1993, a coalition of civil society organisations in Nigeria was formed with the objective of lobbying government officials and actively promoting public awareness of the need for a freedom of information law. Through a process of consultations, workshops and debates on the framework of a freedom of information law, the Media Rights Agenda, the spearhead of the coalition of different stakeholders, produced a draft bill entitled "Draft Access to Public Records and Official Information Act" in 1994. The repressive military regime of the late General Sanni Abacha, erstwhile military head of state, was not receptive of the idea for a freedom of information law.[760]

A revised draft of the proposed bill, entitled Freedom of Information Bill, was presented to the new civilian President, Chief Olusegun Obasanjo by the coalition with a request that he present it to the National Assembly as an Executive Bill for enactment into law. The President declined the request but advised the group to present the Bill directly to the National Assembly.[761] After protracted efforts by the coalition and other interested segments of the society, the National Assembly enacted the Freedom of Information law in November 2006. The Bill was forwarded to the President of the Republic for his assent. The President refused to sign the Bill into law within the thirty days within which to give his assent as provided by the Constitution.[762] Efforts to enact the law were revived soon after the inauguration of

---

760 In June 1998 however, General Abacha died and was succeeded by General Abdulsalami Abubakar who launched a transition to civil rule programme which culminated in the handover to a civilian administration led by Chief Olusegun Obasanjo in May 1999.

761 Ss 58 through 61 of the 1999 Constitution prescribe the legislative process for enactment of a new statute. The first step is for the introduction of a new Bill for an Act into either the Senate or the House of Representatives. The Bill can be presented by a member of the Assembly, the executive branch or a member(s) of the public through the sponsorship of a legislator. It is then referred to the appropriate committee of the legislature responsible for oversight of the matters contained in the Bill. The committee may then carry out a public hearing on the matter if it considers it necessary or deliberate on its own. It is thereafter referred to the plenary assembly of the Senate or House as the case may be for its first reading. The first reading is more of an introductory exercise to acquaint members with the Bill. It is then slated for a second reading at which the legislators will have opportunity to comment, debate and generally make their inputs on the provisions of the Bill. Following this exercise, the Bill is then reviewed by the committee taking into account corrections, amendments and other relevant observations made during the debate. It is then presented for the third and final reading after which it is passed into law by a simple majority in both chambers sitting independently. Where there are differences in the versions passed by both chambers, a joint session is held at which the versions are harmonised and the final copy is sent to the President for his assent. The Bill only becomes an Act after it is assented to by the President and where he refuses to assent, the National Assembly can still pass the Bill into law by virtue of s58 (5).

762 By 23rd April 2007, the deadline for the President's assent to the Bill elapsed and by 29 May 2007, the

the Yar'adua administration in 2007. After 12 years of persistent agitation and advocacy by media proprietors and practitioners, NGOs and Civil Society Organisations (CSOs), the House of Representatives and the Senate passed the FOI Bill on February 24th and March 16th 2011 respectively. The harmonised version was passed by both Chambers on May 26, 2011 and signed into law by President Jonathan on May 28 2011.

1.5 The Freedom of Information Act, 2011

After 12 ardent years of campaign for the right of access to information, Nigeria joined the ranks of countries with a Freedom of Information law on 28 May, 2011, with the signing into law of the Freedom of Information Act, 2011 (FOI Act). With the enactment of the Act, every person resident in Nigeria now has a legal right of access to information, records and documents held by government bodies and private bodies carrying out public functions.[763]

The Act is the product of many years of advocacy by civil society groups and media-based associations such as the Nigerian Union of Journalists (NUJ), Newspaper Proprietors' Association of Nigeria (NPAN) and the Nigerian Guild of Editors.[764] When it was first presented to the National Assembly in 1999 by the Media Rights Agenda on behalf of the coalition of civil society groups that came together to campaign for its passage, the introductory note of the Bill stated that the purpose of the act is to make:

> ... [P]ublic records and information more freely available, provide for public access to public records and information, protect public records

incumbent President, Olusegun Obasanjo ceased to be President by reason of the expiration of his tenure. One of the reasons why the former President, Olusegun Obasanjo refused to sign the then Freedom of Information Bill into law was given by the former Deputy Senate Minority Leader, Senator Olorunimbe Mamora, who alluded to the fear entertained by Obasanjo that "the media would be given too much power to probe the activities of those in government". He made the statement while presenting a paper on "Freedom of Information Act: The Role of the Media in National Development" at the 2011 Press Week of the Rivers State chapter of the Nigeria Union of Journalists in Port Harcourt. See Mamora *Why Obasanjo Refused to Sign FOI Act* [online].

763 S 1 Freedom of Information Act, 2011.

764 MRA *Campaigning for Access to Information* [online].

> and information to the extent consistent with the public interest and the protection of personal privacy, and related purposes hereof.[765]

Although the FOI Act does not expressly repeal the notorious Official Secrets Act, its provisions now override any inconsistent provisions of the Official Secrets Act and supplant any preceding legislation which is inconsistent with the provisions of the FOI Act.[766]

It is commendable that the Act defines "person" broadly so as not to place any limitations arising from the nationality of an applicant who is legally entitled to request and receive information, and also have access to public records.[767] Furthermore, an applicant does not need to prove any specific interest in the information requested or legal standing to make the request.[768] Section 4 of the Act obliges public institutions to make information available to an applicant within seven days, with the possibility of a further seven-day extension. Public authorities or institutions face a fine of up to N500,000 if guilty of "wrongful denial" of information.[769]

A public institution is defined to mean any legislative, executive, judicial, administrative or advisory body of the government. It includes boards, bureau, committees or commissions of the state. Any subsidiary body of those bodies including but not limited to committees and subcommittees which are supported in whole or in part via public funding or which spends public funds and private bodies providing public services, performing public functions or utilising public funds. They

---

[765] After numerous editing and harmonisation of different versions that came into circulation in the 12 years campaign, the final explanatory note states:

> This Act makes public records and information more freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy, protect serving public officers from adverse consequences for disclosing certain kinds of official information without authorization and establish procedures for the achievement of those purposes.

[766] Ss 1 & 28.

[767] Id s 31.

[768] Id s 1(2), (3).

[769] Id s 7(5).

also include all corporations established by law and all companies in which government has a controlling interest.[770] The Act classifies private companies utilising public funds, providing public services or performing public functions as public institutions.[771]

Given its recent enactment, the FOI Act will surely be tested in the courts as the law now provides Nigerians a good opportunity to test the government's commitment to transparency, accountability and good governance. The first judgement arising from an action to enforce the provisions of the Act was delivered recently in the case filed by a non-governmental organisation, Legal Defence and Assistance Project (LEDAP), against the Clerk of the National Assembly.[772]

2. UNREGULATED ACCESS TO PERSONAL INFORMATION AND THE THREATS TO INFORMATION PRIVACY

2.1 Introduction: Increased collection of personal information

Notwithstanding the struggle for access to information highlighted in the preceding paragraphs, there is now a widespread use of information technologies to collect, process and build up databases containing detailed profiles of individuals. The increased collection of personal information has impacted negatively on privacy rights in general, but in particular on information privacy. Automated data collection is now commonplace not only in the developed Western societies, but increasingly also in developing ones. It seems very unlikely these days that a person will go through the day's activities without leaving behind, in diverse computer devices, digital footprints[773] of his or her activities.[774]

---

770 Id s 2(7).

771 Ibid.

772 In the ruling delivered on June 25th 2012, Justice Bilikisu Aliyu of the Federal High Court, Abuja, ordered the Clerk of the National Assembly to release to Legal Defence and Assistance Project (LEDAP), a non-governmental organisation within 14 days, details of the salary, emolument and allowances collected by Nigerian legislators between 2007 and 2011. LEDAP had earlier written to the Clerk of the National Assembly for the information on the earnings of the legislators and demanded refund of over-payments but the request was ignored, leading to the suit. See Anaba June 26th 2012 *Vanguard.*

773 Kang 1998 (50) *Stan L Rev* 1193. A person's digital footprint is everything on the Internet that is about the

In the past, for example, going to a restaurant and ordering a meal did not require one to reveal one's identity; one simply sat down, ordered a meal and after eating, paid in cash for the meal. It was not possible for the restaurant to identify the patron in such a direct transaction even if the patron was a regular user of the restaurant, unless the information was knowingly divulged by the patron. Today, however, with the proliferation of credit and debit cards, barcode scanners, cameras and other tracking devices, dining at a restaurant, ordering a pizza from home, buying goods in a store, paying for one or other service, or making a telephone call, all leave digital trails which can be used to identify a patron. For example, paying for a meal at a restaurant by means of a credit or debit card elicits two information processes; firstly, the point-of-sale (POS) terminals will calculate the cost of the food and drinks consumed; secondly, it will detect if there is any pattern in the customer's dining habits. Undoubtedly, credit and debit cards ease payments in commercial activities, particularly e-commerce transactions, but they also open users of the cards to subsequent targeted marketing made possible by the data captured in the POS terminals.[775]

The use of information technology networks for commerce creates information trails that allow customers' transaction information to be easily tracked, collected, and compiled, thereby providing information brokers (as well all other interested persons), with the personal details of people's lives. Supermarkets and other retail establishments use scanners that allow purchases to be tracked. Bank and credit card companies collect information about the shopping and payment histories of their customers. Insurance companies, doctors and hospitals maintain vast amounts of personal information about their clients and patients. Visiting a website for an online

---

person. This could be:

- a profile on Facebook or Linkedin,
- photographs that the person, his/her friends or family have posted online, or
- anything the person has written or has been written about him or her, for example, on discussion boards, blogs, or in articles.

[774] Id at 1198-1199. Consider for example, Jerry Kang's graphic description of how we leave digital footprints when we visit a shopping mall in real space or in cyberspace. In cyberspace, every interaction is captured and according to Kang, "[a]ll these data generated in cyberspace are detailed, computer-processable, indexed to the individual, and permanent." See also Agre "Personal Information in the Digital Age".

[775] Ibid.

purchase or placement of an order for goods or services is an open invitation to the website to mine as much personal information about the user as possible.[776]

An increasing amount of personal information now makes up the records maintained by Internet Service Providers (ISPs), telephone and telecommunications companies, hotels, banks, websites, employers and many other private entities. Many of these holders of personal information have either aggregated them or will in the future do so and thereby create massive databases. The public's awareness of the use and potential for misuse of personal information in these aggregated databases has heightened in recent years, with people demanding the right to control the use of information they provide about themselves, whether to corporations, governments or any other organization. Whenever a person gives out his or her personal information, either willingly or mandatorily, there is a loss of information privacy because information privacy is essentially control over access to personal information.[777] One way to reassert a measure of control over our personal information is to have access to such information held by others about us.

In this respect, we find a complementarity between the interests in freedom of information and information privacy. This is however offset by the fact that increased collection of personal information, occasioned by increasing freedom of access to information globally and aided by technology, often results in misuse of such information.[778] In seeking to reconcile freedom of access to information with information privacy, it is necessary to first examine the roles of technology and

---

776 See n 773 at 1198-1199.

777 See n 773. Kang adopted the definition of information privacy given by the Clinton Administration's Information Infrastructure Task Force (IITF) as "an individual's claim to control the terms under which personal information - information identifiable to the individual - is acquired, disclosed, and used" (at 1205). See also Fried 1968 (77) *Yale L J* 475 at 482.

778 Ibid. The misuse of personal information inevitably results in the erosion of the values of information privacy. Kang identified three values that characterise information privacy. They are: i. avoiding embarrassment, ii. constructing intimacy and, iii. averting misuse. He argues that in many different cultures, the disclosures of certain behaviours or actions will embarrass the individual - even when the behaviour or action is neither blameworthy nor stigmatized. Secondly, unauthorised disclosure of personal information can hinder the construction of intimate relationships and hinder the sharing of personal experiences as it would create a sense of being under observation under which spontaneity, so essential to building up intimate relationships, is stifled. Thirdly, when personal information is misused, it places the person to whom it relates in a vulnerable position and therefore open to harassers and stalkers or identity thieves (Kang 1212-1217).

commerce in the collection of personal information on the one hand, and the threats that these activities pose to information privacy. While public access to government-held information[779] will enhance democracy, it may also significantly interfere with personal information privacy interests. These interests inevitably give rise to tensions or conflicts between the demands for the control of personal information and the demand for greater access to information.

2.2 The use of technology in the collection of information and record-keeping

It was in the late 19th century that record-keeping entered the mechanisation age with the invention of punch cards and an electromechanical equipment to "read" and process them. For data to be processed and stored electronically, it must be readable, thus data that are collected in non-digital form must be converted to digital format by an electro-mechanical device. This device was invented by Herman Hollerith[780] who first used it in the US census of 1890. It provided a dramatic decrease in the time it took to process the census data, compared with previous manual methods.

The development of computers from the 1940s onwards and their application to business data processing and record keeping, marked a quantum leap in record keeping technology and set the stage for new advances in collection, storage and processing of information.[781] The introduction of computing technology into the process of gathering, sorting and storage of information has had a most significant impact not only on record keeping generally, but perhaps more so in the way the

779 The South African Promotion of Access to Information Act, 2000 allows access not only to government-held information, but also information held by private companies. The Nigerian Freedom of Information Act, 2011 grants access to information, records and documents held by government bodies and private bodies carrying out public functions.

780 Huskey and Velma 1976 (C-25) No 12 *IEEE Transactions on C*omputers 1190-199.

781 Computers were first introduced into commercial activities in the 1960s, in the banking industry in the USA with the Electronic Recording Machine Accounting (ERMA). Prior to this, banks had been swamped with the growing volume of cheques that needed to be processed. Computers helped the banks to speed up the sorting process and in no time, the commercial use of computers quickly spread as companies in a variety of industries introduced them to their book keeping and accounting functions, administer payroll, create management reports, and schedule production. In the 1970s and 1980s, businesses extended their computing usage beyond the company's walls, by sending and receiving information with business partners and suppliers electronically via EDI (Electronic Data Interchange). See Winn *The Emerging Law of Electronic Commerce* ch 32.

information is used.

Data processing is no longer limited to simple counting and collation of raw data or information; it now includes virtually any desired processing operation.[782] The most critical factor that accelerated the deployment of computer technology in the collection, processing and storage of information was the introduction of optical character readers called scanners that recognise a variety of printing fonts and convert printed text into computer-readable form.[783] The elimination of the need to transcribe information manually signalled the exponential growth in the quantum of data collection around the world, but particularly in the industrial world. Improvements in computer hardware over the years have made their use easier and their utilisation more efficient. In 1994 for example, the Intel 486 microprocessor chip was able to carry out 54 million calculations per second. Gordon Moore,[784] the co-founder of Intel had predicted in 1965 that by continually making transistors increasingly smaller and more tightly packed together, there would be a corresponding increase in computing power and data storage which would double every year. This prediction, known as Moore's Law, has proved to be reasonably accurate in the last three decades.[785]

In the early 1970s, database management programmes became available to large businesses, and by the 1980s they were affordable for use in micro computing systems.[786] The bulk of information stored in databases around the world is personal information and a great deal of it is generated as a result of our increasing reliance on the use of information and communication technologies. These technologies in turn have increased the variety of transactions that generate records about individuals, called transaction-generated information (TGI).

---

782 See n 780.

783 Ibid.

784 Moore's original statement of what later became "law" can be found in his publication "Cramming more Components onto Integrated Circuits", in Moore 1965 (38) No 8 *Electronics* 114.

785 Fuchs 2001 (145) No 1 *Proc Am Phil Soc* 46.

786 Safier *Between Big Brother and the Bottom Line* [online].

A very critical implication of transactions-generated information is the fact that they can be readily utilised for multiple purposes, some of which may not be related to the transaction or events that generated them.[787] For example, information collected by a retailer of wines, may end up being used by a purveyor of pornographic materials for marketing purposes without the consent or knowledge of the individual to whom the information relates. Furthermore, the ability of computer technology to correlate the information stored in its database has resulted in the ability of governments and businesses, particularly the latter, to profile large classes of individuals thus enhancing the business or government's ability to make more informed decisions about individuals. Businesses can more efficiently target potential markets as a result of the profiling results obtained from their databases.[788]

2.2.1 Historical development of the use of technology for collection of information

The trend towards the collection and collation of information did not begin in the 21st century. It began as early as when man first began to keep a record of his physical assets. Some of the technologies for keeping record are as old as the practice itself. The technologies were largely dependent on the state of civilization in the society. Record keeping activities in ancient societies saw a gradual progression from the collection of information about natural and astronomical events in aid of religious activities, to the collection of information about people and their environment, to population and then to land holdings, etcetera, to aid in economic activities.[789]

A good example is the case of William the Conqueror of England. In the course of his reign in the eleventh century, he caused information to be collected about the number of people in his domain, their land holdings, cattle, and the extent of his own land holdings in order to determine the extent of his wealth and the taxable subjects and accruable income to his kingdom. All the information collected was compiled in

787 Solove 2006 (154) No 3 *U Pa L Rev* 477. See also Kang n 737 above.

788 Ibid.

789 Privacy Protection Study Commission "Technology and Privacy" 5 [online].

the Domesday Book.[790] The information contained therein became a source of knowledge and power; knowledge because he had a fair idea of what income was due to him in the form of taxes and the number of taxable subjects in his kingdom, and power because, with such knowledge, all the subjects whose information were contained in the Book were exposed to his coercive capacity – there was literally no hiding place for them. Information is power, therefore, as Froomkin[791] asserts, the collection and collation of personally identifiable information are means of acquiring power, usually at the expense of the data subject.

In the example of William the Conqueror, his agents and assigns went about the realm collecting the requisite information from the subjects by means of oral interviews and personal observation; the information collected were stored in ledgers and eventually transcribed in the Domesday Book. The whole process was long, slow and laborious as it could only be accomplished by reliance on pen, ink and vellum. However, the moment the raw data was collated and inscribed in the Book, the totality of information contained in the Book became sources of power and control on the one hand, and an economic resource on the other, enabling the king's servants to levy taxes. To this day, the collection and collation of personal information have continued unabated, with governmental authorities being at the forefront of such collection and collation.

For about 900 years since the compilation of the Domesday Book, the collection, collation, storage and use of personal information followed the pattern used by the agents of William the Conqueror – the slow and laborious process of oral interviews and manual recording of the raw data into ledgers or fact sheets and later collation of the data and storage in record books. Record-keeping, that is, the collection and processing of information, have until recently followed the same pattern of question and answer interaction between the person seeking the information and the one supplying it.[792] This was the most basic means of collection until the introduction of application forms. Even with the use of application forms, information was

---

790 Domesday Book [onli ne].

791 Froomkin 2000 (52) *Stan L Rev* 1464.

792 Ibid n 790 above.

transferred from the giver to the receiver by writing, or orally.

2.3 The marketplace for trading personal information

Just as the "database" compiled by William the Conqueror's agents later translated into increased revenue into his coffers, so also the information contained in modern computer databases have acquired a monetary value of their own. The information economy is based upon the premise that information has economic value and therefore requires an information marketplace in which such value can be exchanged.[793]

The existence of such a marketplace for information was highlighted by the Information Commissioner of the UK in a report to Parliament.[794] According to Richard Thomas, the Information Commissioner, "[p]ersonal information has a value - whether it is the embarrassing secret of a celebrity, a politician or someone else in the public eye or the whereabouts of a private individual who it is thought owes money."[795] He referred particularly to the financial services industry, insurance companies, local authorities, the media and those making use of private investigation agencies as active participants in the illegal trade.[796]

The buyers of personal data, such as journalists, mostly seek information about celebrities and look for scoops on news events; the insurance and finance companies buy information to enable them to trace debtors. Rothfeder[797] asserts that about five billion records in the US describe each resident's whereabouts and other personal information. He also claims that such information is moved from one computer to another about five times a day. According to him:

---

793 Cohen 2001 (89) *Geo LJ* 2029.

794 Information Commissioner's Office *What Price Privacy? The Unlawful Trade in Confidential Personal Information* 1.

795 Id at 3.

796 S 55 of the UK Data Protection Act 1998 makes it an offence to obtain, disclose or 'procure the disclosure' of confidential personal information 'knowingly or recklessly', without the consent of the organisation holding the data.

797 Rothfeder *Privacy for Sale* (1992) 22-23.

> Information about every move we make - buying a car or a home, applying for a loan, taking out insurance, purchasing potato chips, requesting a government grant, getting turned down for credit, going to work, seeing a doctor - is fed into ... databases owned by the credit bureaus, the government, banks, insurance companies, direct marketing companies, and other interested corporations.[798] The data in these databases are then sold to a nation-wide network of databanks and information resellers.

2.3.1 New business models: their influence on the collection of personal information and threat to information privacy

In the last decade, new business models have been established and have achieved public prominence as a result of harnessing the potentials of the growing information economy. The growth of the Internet, advances in e-commerce technology, the outsourcing and off-shoring of many business activities and the restructuring of the financial services industry around the world have all contributed to the success of the new business models.[799] These new models of business thrive in the Internet environment, they are operationally different from the mortar and bricks models of the industrial era and they are largely based on the notion of greater customization of services and products based on personal information collected from the Internet.[800] They require large quantities of personal information so that appropriate customization and targeting can be used.

The demands for greater economic efficiency and the availability of more personal information, coupled with advances in computer and telecommunications technologies, have made it easy for marketers to use personal data in their targeted

---

798 Ibid.

799 Teece 2010 (43) *LRP* 174. Some of the companies that were established in the last decade and achieved international prominence are Google Inc., Facebook, MySpace, etc.

800 For example, a *World Street Journal* investigation about businesses, the Internet and collection of personal information, found that the fastest growing businesses on the Internet are the ones engaged in the business of spying on users of the Internet and collecting their personal data. See Angwin July 30th 2010 *The Wall Street Journal*.

or direct marketing drives.[801] By using personal data that has been collected, collated and stored in a database, they can more efficiently create promotional programmes targeting the right type of customers and/or prospective customers.

Loyalty programmes, such as the frequent-flyer schemes set up by many airlines, are direct results of the use of personal data to target specific, identifiable individuals. These programmes provide a rich pool of direct marketing targets.[802] The marketing industry considers direct marketing schemes such as loyalty programmes, as the means to better understand their customers; privacy advocates, however, consider these schemes as threats to privacy. Loyalty programmes have been described as having the key purpose of collecting personal information.[803] A great deal of this collection takes place in cyberspace. Jerry Kang argues that:

> [D]ata collection in cyberspace produces data that are detailed, computer-processable, indexed to the individual, and permanent. Combine this with the fact that cyberspace makes data collection and analysis exponentially cheaper than in real space, and we have what Roger Clarke has identified as the genuine threat of "dataveillance".[804]

According to Culnan and Armstrong,[805] consumers willingly disclose personal information in exchange for some apparent benefits. They argue that consumers are also likely to provide personal information if they believe they have control over the use of the information provided, the information requested is relevant to the service or product desired and it is likely to create valid inferences about their preferences.

Indeed, a significant portion of the personal information available in both cyberspace and real space has been willingly disclosed by the persons they refer to. Such

---

801 Ibid.

802 According to the Irish Data Protection Commissioner, direct marketing involves a person being targeted as an individual, and the marketer attempting to promote a product or service, or attempting to get the person to request additional information about a product or service. See Data Protection Commissioner of Ireland *Frequently Asked Questions* [online].

803 Stoddart *Privacy in the Marketplace* [online].

804 See n 773 at 1261.

805 Culnan and Armstrong 1999 (10) No 1 *Organization Science* 106.

personal information can be found in banks, in doctors' clinics, in schools, offices, churches, political organisations, and even recreational facilities. People give out personal information about themselves, very often quite willingly, but sometimes they have no choice in the matter. In the past, however, most of this data was usually on paper and kept in scattered locations. Retrieving such data was a daunting task which benefited the privacy of the individual. Today, however, a vast amount of such personal information about individuals and private groups has been computerised and can be retrieved in an instant. There are also many companies that are in the business of collecting and reselling personal information.

2.3.1.1 The data brokerage industry

The growth of the Internet has made it possible for businesses to deliver value to their customers by extracting value from information services that were not possible decades ago. The biggest leverage that the Internet has given to the new business models in operation today is that it has allowed individuals and businesses to have easy access to vast amounts of data and personal information. Not only is the Internet an easy source of digital data, it is also a new channel of distribution of digital goods and services.

A business model reflects the management's hypothesis about what customers want, how they want it, and how the enterprise can organise to best meet those needs, get paid for doing so, and make a profit."[806] According to Teece, it defines the manner by which the enterprise delivers value to customers, entices customers to pay for value, and converts those payments to profit.[807]

One way to become more competitive in today's information-driven economy is to be more efficient in terms of targeting advertising or direct marketing messages at potential buyers. To achieve this, more detailed data about the potential buyer or customer is required. This is where the information brokers have a role to play; they acquire huge volumes of data from diverse sources, aggregate the data and produce

806 See n 799 at 172.

807 Ibid.

databases containing as much detailed information about specific individuals as possible.

This business model has been particularly successful in the US, where a technologically advanced marketplace and a largely unregulated right of access to personal information in public records have encouraged the development of the data brokerage industry.[808] The industry is made up of diverse companies engaged in information brokerage, information re-sale and other information solution services. They collect personal and non-personal information from diverse sources, collate, store, perform data mining and analysis of the data to glean more valuable information and sell the aggregated information. Their customers include private sector retail, insurance, health management, marketing and manufacturing businesses as well as government agencies especially law enforcement and national security agencies.

These companies fall under two broad categories: the first group is made up of reference service providers. They sell profiles and other information reports that contain confidential personal information about individuals; these reports may be required for background checks, credit worthiness reports, etc. The second group is made up of data mining companies who sell personal information that has been collected and refined to the point of being able to make distinctions pertaining to individuals with respect to their age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries and vacation dreams.[809]

Some of the leading companies in the information brokerage industry are mainly US-based companies such as Acxiom, Choicepoint and Lexis-Nexis. For example, Acxiom is one of the biggest data brokers in the world; it collects, collates, aggregates and sells information about consumers' offline, online and mobile activities for marketing and other purposes. It is said to have amassed the world's largest commercial database of consumers; the company's database contains information on

808 Solove and Hoofnagle 2006 (2006) No 2 *U Ill L Rev* 359.

809 Editorial Staff June 20, 2012 *The Week*.

about 500 million active consumers worldwide, with about 1,500 data points per person.[810] The company started in 1969 as Demographics Inc., "… using phone books and other notably low-tech tools, as well as one computer, to amass information on voters and consumers for direct marketing."[811] From then till now, it has collected and refined data on more than 190 million people and 126 million households in the US alone and about 500 million active consumers worldwide. It has more than 23,000 servers that engage in the collection, analysis and storage of more than 50 trillion data transactions that it monitors in a year.[812] According to Robert O'Harrow,[813] Acxiom is "a billion-dollar player in the data industry, with details about nearly every adult in the United States."

It also uses predictive analytics[814] to forecast how consumers will act, what they will buy and how companies can persuade them to buy their products. It collects its data from public records, surveys filled out by consumers online and offline, personal information posted on social media networks such as Facebook and other diverse sources of information, which it then sells to banks, retailers, and other buyers.

2.3.1.2 Internet search engines

Search engines collect and process vast amounts of data, including data gathered by technical means, such as cookies. They are programmes designed to point Internet users to a list of relevant Web sites that correspond to a user's request for

---

810 Singer June 16, 2012 *The New York Times*.

811 Ibid.

812 Ibid.

813 O'Harrow *No Place to Hide* 34.

814 Predictive analytics is the use of business intelligence data for forecasting and modelling; it involves the use of quantitative methods to derive insights from data, and then drawing on those insights to shape business decisions and, ultimately, improve business performance. Instead of looking backward to analyse what had already happened, predictive analytics helps business executives to predict future patterns and events. See Rich and Harris *Predictive Analytics* [online]. According to Alex Guazzelli, predictive analytics has been around for many decades as a discipline, mostly in academia. Its relevance in industry increased as a result of the increasing amount of data being captured from people (for example, from on-line transactions and social networks) and sensors (for example, from GPS mobile devices) as well as the availability of cost-effective processing power. He notes that predictive analytics is able to discover hidden patterns in data that the human expert may not see. See Guazelli *Predicting the future* [online].

information about some topic or subject. Search engines can be used to locate information on a variety of topics – from academic research, to recreation, travel, commerce, etcetera.[815] Data collected can range from the IP address of individual users to extensive histories of past searching behaviour or data provided by users themselves when signing up to use personalised services.[816]

Search engines can also be used to locate personal information about individuals; some of the personal information that are accessible to search engines can be found in public records that are freely available online while some are contained in commercial databases maintained by information brokers such as Acxiom and Choicepoint,[817] which can be accessed only by payment of fees to the database owners. Tavani[818] makes the point that some information about persons currently accessible online have been made available inadvertently and in many cases, such information may have ended on the Internet without the knowledge and consent of the person or persons affected. The fact that an individual may be unaware that his or her name is among those included in one or more databases accessible to search engines raises privacy concerns.

Certain types of information about individuals, which were once difficult to find and even more difficult to cross-reference, are now readily accessible and collectible through the use of Internet search engines.[819] By entering the name of an individual in a search engine programme's entry box, search engine users can potentially locate and retrieve information about that individual. Search engines can also search through archives of news-groups, such as Usenet, on which online users post and retrieve information.

According to Tavani, one such group, DejaNews, is set up to save permanent copies

---

815 Tavani 2005 (3) No 6 *IRIE* 40.

816 Art 29 Data Protection Working Party *Opinion* 1/2008 on *Data Protection Issues Related to Search Engines.*

817 See par 2.3.1.1 above.

818 See n 815.

819 Wright and Kakalik 1997 (27) No 4 *C&S* 22-25.

of new postings. It thus provides search engines with a comprehensive searchable database and because the various news groups contain links to information posted by a person, they can provide search engine users with considerable insight into the interests and activities of persons who contribute to such online discussion groups. Tavani argues therefore that not all of the personal information currently included on Web sites accessible to search engines was necessarily either placed there by the persons themselves or explicitly authorized to be placed there by those persons.[820] Apart from the privacy concerns raised by the accessibility of personal information to search engines, there is also the issue of the security implications of unregulated access to personal information through search engines. This twin problem was highlighted in the case of Amy Boyer who was murdered in 1999 by Liam Youens, who obtained vital information about her through the use of an Internet search engine.[821]

The Article 29 Data Protection Working Party of the EU, while recognising the usefulness of search engines and their importance in the daily life of individuals using the Internet and other information retrieval technologies, has noted that European data protection law applies not only to the index of search results generated by search engines (that is, content data), but also to other specific situations involving search engines, such as if they offer a caching service or specialise in building profiles of individuals. In its opinion on *Data Protection Issues Related to Search Engines*,[822] the Working Party, while seeking to strike a balance between the legitimate business needs of the search engine providers and the protection of the personal data of Internet users, identified a clear set of responsibilities under the *Data Protection Directive*[823] for search engine providers as

---

820 See n 815.

821 Amy's mother, Helen Remsburg, filed an invasion of privacy lawsuit based on "commercial appropriation of personal information", in addition to a "wrongful death" lawsuit, against Docusearch, the commercial information broker who supplied the killer with Amy's personal information that enabled him to gain access to her and kill her. The facts and legal arguments in the case are well captured in the *amicus* brief filed by the Electronic Privacy Information Center (EPIC) in support of the mother's case. See EPIC *Amicus Curiae brief in Estate of Helen Remsburg* [online].

822 Article 29 Data Protection Working Party *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, adopted on 4th April 2008.

823 *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*. OJ L

controllers of user data.

A key conclusion of the Opinion is that the *Data Protection Directive* generally applies to the processing of personal data by search engines, even when their headquarters are outside the European Economic Area (EEA), and that the onus is on search engines in this position to clarify their role in the EEA and the scope of their responsibilities under the Directive. The Working Party makes it clear that the *Data Retention Directive*[824] is not applicable to search engine providers and that personal data must only be processed for legitimate purposes. The Working Party concludes that search engine providers must delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for. Search engine providers must also seek the consent of the users of their services for all planned cross-relation of user data and user profile enrichment exercises. The Working Party also noted the obligation of search engine providers to clearly inform their users of all intended uses of their data and to respect the users' right to readily access, inspect or correct their personal data in accordance with Article 12 of the *Data Protection Directive*.

2.3.1.3 Social networking websites

Boyd and Ellison define a social networking website as a web-based service that enables individuals to "construct a public or semi-public profile within a bounded system; articulate a list of other users with whom they share a connection; and view and traverse their list of connections and those made by others within the system."[825] Millions of people across the world use social networking sites like Facebook, Twitter and MySpace to meet, chat and send messages to one another online. Although the features of the various social networking sites are different, they all facilitate the sharing of information among their users by allowing their users to post text, images,

---

281, 23/11/1995 P. 0031 0050.

824 *Directive 2006/24/EC of the European Parliament and of the Council 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*, OJ L 105, 13.4 (2006).

825 Boyd and Ellison 2008 (13) No 1 *JC-MC* 210.

videos, and other information to their profiles. The provision of, and sharing of personal information is very fundamental to the formation of social networking websites. In a sense, it is the cement that holds the whole infrastructure of such websites together. The shared information is available to all manner of people with various motivations for seeking the readily available information which can then be put to diverse uses.

According to Spinello,[826] Facebook, one of the most popular social networking websites, encourages users to reveal to the public as much information as possible because the social networking business model is based on a clear *quid pro quo*: millions of people expose highly personal information about themselves in exchange for the ability to communicate with their friends, family members, and colleagues. The lower the level of privacy, the more personal information is available to be mined for the benefit of its business interests. He argues that this business model sets the stage for complex privacy trade-offs; in order to monetize this "free" technology, Facebook uses its consumer data to deliver targeted online adverts and marketing messages. The types of personal information provided by users of these websites usually include information about their true names, location, work, hobbies, and friends. Apart from the personal information members post about themselves, their friends may also reveal information about them which may expose them to some danger such as sexual predators or cyber-stalkers and other malicious users of the websites.

Because younger people are less concerned about information privacy, they are more willing to disclose their personal information online. The personal information they reveal very often attracts sexual predators and exposes the young users to other dangers such as cyber-stalking.[827] There have been many reports of sexual predators locating their victims through social networking sites.[828]

---

826 Spinello 2011 (16) No 12 *IRIE* 43.

827 Huffaker and Calvert 2005 (10) No 2 *JCMC* 63 [online].

828 For example, in 2011, the BBC carried a news report about a young man who admitted abusing girls he met through Facebook. The man, Jake Ormerod, 20, admitted 13 charges at Exeter Crown Court relating to eight girls as young as 13. He was said to be part of a paedophile gang who used the social networking site to target victims. He was sentenced to 10 years in jail. See BBC News "Facebook sex abuser" [online]. See

Other features of the social networking websites that cause concern, particularly with regard to information privacy, include: the availability of users' personal information to third parties for commercial, surveillance or data mining purposes[829]; the use of facial-recognition and tagging software to automatically identify persons in uploaded photos[830]; the use of "cookies" to track online user activities while on the websites or after they have left.[831] The availability and easy access to personal information on social networking websites exemplifies the negative impact that unregulated access to personal information has on information privacy.[832]

2.4 Other threats to the privacy of personal information

While acknowledging the importance of privacy as a fundamental right, governments and private sector organisations have nevertheless in recent years intensified surveillance into almost every aspect of the citizens' lifestyles. They argue that surveillance is necessary to maintain law and order and to create economic

---

also the CNN coverage of the rape and murder of a young Nigerian lady by two young men she befriended on Facebook. The suspected killers targeted and lured her to Lagos because they believed she would be carrying large amounts of cash. In Lagos, she was taken to a hotel, drugged, and sexually assaulted, before being murdered. Duthiers *CNN News* "Facebook 'stalkers' face trial" [online].

829 Dignan "FBI, Feds collect Facebook, social media data; why are you surprised?" [online]

830 A report by ABC News reporter, Ki Heussner, on tracking of users of social networking websites, highlights an application named "Creepy" that can track a person's location on a map using photos uploaded to social network sites Twitter or Flickr. The report notes that anybody using the application can search for a specific person and then find their immediate location. "Creepy" works because modern smart phones are able to embed the longitude and latitude coordinates of the location where the photo was taken into the photo and the information is automatically sent to the website along with the uploaded photo. "Creepy" is able to use the uploaded information to track the most recent location of the person in the photograph. This geo-tagging ability of the application clearly poses potential threats to users who share their information with a large group of followers. See Heussner March 1, 2011 *ABC News*.

831 For example, when a user logs into Facebook, the site sends a cookie to the user's browser which is disabled only when the user logs out of his or her Facebook account. As the user visits various web sites, the "Like" architecture, in the form of a small widget or button, will report back to Facebook whether or not the user has clicked on the Like button (even if the user doesn't click on this button, Facebook knows that the user has been to this site and looked at this item). Amir Efrati argues that this social networking widget provides a history of a user's Web-browsing habits that can be linked to personally identifiable information. He notes that the Like architecture has the potential to be a powerful mechanism for behavioural advertising. See Efrati May 18 2011*Wall Street Journal B2*.

832 See Tavani and Moor 2001 (31) No 1 *C&S* 6-11; Moor *Towards a Theory of Privacy for the Information Age* 407- 417.

efficiency, and that privacy rights in general must remain subject to constraints of fiscal and public interest.[833] The tremendous scientific and technological developments that have taken place in recent years have made the widespread use and abuse of electronic surveillance techniques possible.

Despite the convenience and the widespread popularity of cellular and other wireless telephones, people have become concerned that these modern systems of communication are insecure. The very nature of their architecture enables them to be used as instruments of non-physical intrusion into the privacy of their users.[834] Such non-physical intrusion may be effected by surveillance devices which do not need to physically intrude on property or come close to the target. These devices operate by intercepting at a distance, information transmitted by satellite, microwave and radio, as well as mobile telephone transmissions.

Aural surveillance generally refers to the surreptitious eavesdropping, either directly by ear or by means of some technical device such as a wiretap, microphone or amplifier, of conversations, or the preservation of such conversations by a recording device.[835] Wireless transmissions are particularly susceptible to eavesdropping by means of electronic surveillance.[836] The two main ways by which personal information communicated through the electronic medium are interfered with are described below.

2.4.1 Monitoring and interception of electronic communications

In the aftermath of the September 2001 terrorist attacks in the US, many countries have enacted or amended their wiretapping and electronic surveillance laws to give wider powers to police and national security agencies to intercept oral, telephone,

833 Davies March 2001 *UNESCO Courier* 18.

834 Dempsey 1997 (8) No 1 *Albany Law J Sci Technol* [online].

835 The Law Reform Commission of Hong Kong *Consultation Paper on Civil Liability for Invasion of Privacy.*

836 See n 834. According to Dempsey, wireless eavesdroppers invade not only the privacy of the person who is using a wireless phone, but also of anybody else who is in the conversation using an ordinary landline telephone.

fax, telex and e-mail communications.[837] E-mail is easier to intercept than regular mail. Since e-mail messages are often stored with a service provider for a period of time before they are read by the intended recipient and perhaps even after they are read, they are thus more vulnerable to interception.

Electronic surveillance erodes the power of individuals to control information about themselves and the terms on which it is shared. Unlike the traditional search warrant which authorizes only one intrusion at a time, electronic surveillance involves an on-going intrusion into a person's private sphere.[838] Dempsey argues that the announcement of authority and purpose is considered essential in the course of executing the traditional search warrant. This enables the person whose privacy is being invaded, to observe any violation in the scope or the conduct of the search and immediately seek a judicial order to halt or remedy any violations. In contrast, wiretapping is conducted surreptitiously.[839]

Wiretapping and electronic surveillance are highly intrusive forms of investigation. Major international agreements on human rights seek to protect the individual from unwarranted invasive surveillance; international human rights law requires that everyone should have their reasonable expectation of privacy respected and protected.[840] In most democratic countries, the interception of communications is usually initiated by law enforcement or national security agencies after due approval by a judge or some other independent magistrate or high level official and generally only for serious crimes.[841]

---

837 Perhaps the most notorious of these laws is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT) of 2001 Act which was enacted into law by the American Congress in the wake of the terrorist attacks of September 11, 2001. The Act expanded governmental authority to monitor Internet traffic, to compel disclosure of information contained in public and private records if approved by the judicial branch, and to share information so collected with any Federal law enforcement, intelligence, protective, immigration, national defence, or national security official in order to assist the official in the performance of his official duties.

838 See n 834.

839 Ibid n 834.

840 See art 12 of the 1948 *Universal Declaration of Human Rights* and art 17 of the *International Covenant on Civil and Political Rights*. See also. Ramage *Privacy: Law of Civil Liberties* 43.

841 In Nigeria for example, the NCC has now introduced a Draft Lawful Interception of Communications Regulations for public comment. Until the draft regulations are formally adopted by the NCC, the position at present is that there are no clear rules governing interception of communications in Nigeria. See NCC *Draft Lawful Interception of Communications Regulations* [online].

2.4.2 Eavesdropping

Eavesdropping on private conversations is an intrusion on the solitude and seclusion of the parties to the conversations. It enables the eavesdropper to pry into another person's private affairs and thereby constitutes an invasion of privacy. The objection to the interference with privacy has more to do with the loss of control over what, when and how information about the individual is disclosed. According to Raymond Wacks,[842] overhearing or observing an individual in circumstances where he has reasonable expectations of privacy is objectionable even though the person overhearing or observing does not acquire any sensitive or intimate information about the person overheard.

In the South African case of *S v A,*[843] the court held that eavesdropping and electronic surveillance by private detectives during matrimonial disputes may result in a criminal invasion of privacy if the methods used were unreasonable. Also, in *Klein v Attorney-General WLD*[844] the restoration of computer information that had been deleted or erased by its owner and the handing of it over to the state for use in criminal prosecution, was held to be a violation of the owner's privacy right. Similarly, in *Janit v Motor Industrial Fund Administrators (Pty) Ltd*[845] the stealing of tape recordings of confidential business meetings and offering them to a third party was held to be an unlawful invasion of privacy.

In *Halford v United Kingdom*[846] a former British Assistant Chief Constable, Allison Halford complained that following her sex discrimination complaint against the police, her office phone had been tapped. The British government asserted that this was an entirely lawful and proper activity as it fell outside the protection of article 8 of the European Convention. Halford maintained that it breached her right of privacy under the said Convention. The European Court of Human Rights agreed, and ruled

842 Wacks *Privacy* 247-248.

843 1971 (2) SA 293 T at 297.

844 1995 (3) SA 848 (W).

845 1995 (4) SA 293 (A).

846 24 EHRR 523, 25 June 1997.

that the police had acted improperly in tapping Ms Halford's phone. It referred to its case law which had established that telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8.[847] The merging of voice, data and images in digital communications systems has generated large quantities of transactional data that can be readily collected and analysed.[848] The explosion in the amount of personal information transmitted and stored electronically has inevitably resulted in greater exposure to intrusion, interception and misuse.

3. BALANCING THE RIGHT TO INFORMATION AND THE RIGHT TO PRIVACY

3.1 The value of information privacy

Information privacy promotes distinct societal values by providing a context that allows, or creates the conditions in which individuals may pursue their personal development and interact or engage with one another in the pursuit of diverse ends.[849] In a similar vein, the freedom of citizens to choose what information they share with others is one of the fundamental differences between totalitarian states and free societies. In the words of Charles Fried,[850] privacy "is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves." Similarly, Westin defines privacy as the "claim by individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[851]

---

847 See *Huvig v France* 12 EHRR 528 1990; *Silver v United Kingdom* 3 EHRR 475 1980.

848 See Reidenberg 1992 (44) No 2 *Fed Comm L J* 195.

849 See Perez-Albuerne and Friedman 2001 (19) No 3 *JMJC& IL* 449-450. Perez-Albuerne and Friedman, in discussing the relationships that are enabled by information privacy, argue that relationships between contracting or negotiating parties are not likely to form without the assurance that the parties involved will be able to exercise control over access to, and the dissemination of, information about themselves and the nature of their relationship.

850 Fried 1968 (77) No 3 *Yale L J* 482.

851 Westin *Privacy and Freedom* 31-32.

These views exemplify the discourse on privacy and privacy rights in the US, which tends to focus mostly on the benefits the rights have for individuals *qua* individuals. These benefits are usually cast in terms of securing (or helping to secure) individuality, autonomy, dignity, emotional release, self-evaluation, and inter-personal relationships of love, friendship and trust.[852] According to Bennett and Raab,[853] this perspective on the value of privacy also obtains in other developed countries; it is an integral feature of what the authors term the "privacy paradigm" – a set of liberal assumptions informing the development of data privacy policy in the bulk of advanced industrial states.[854]

Information privacy essentially refers to the right of individuals to control information about themselves - to keep it secret or to share it with others only as they see fit.[855] The key element of information privacy is therefore control and/or knowledge over who has access to such personal information. The acquisition of private information by a second or third party, in the absence of consent or knowledge of the individual concerned, is a breach of information privacy. Such a breach signifies loss of control over information which can compromise the context that enables the individual to maintain a sense of autonomy.[856]

People may be willing to allow the invasion of some aspects of their privacy in order to obtain benefits like medical treatment or a driver's licence. They recognise that governments need to collect personal information for purposes such as tax collection

852 See Bygrave *Data Protection Law: Approaching Its Rationale, Logic and Limits* 133–134.

853 See Bennett and Raab *The Governance of Privacy: Policy Instruments in Global Perspective* 13-25. In Germany however, the value of data privacy norms is mostly seen to lie in their ability to secure the necessary conditions for active citizen participation in public life thereby securing a flourishing democracy. According to Anna-Bettina Kaiser, the German Federal Constitutional Court invented the famous right to informational self-determination (*Recht auf informationelle Selbstbestimmung*), i.e., the right of individuals to decide whether or not to disclose personal information and also to decide about their usage, subject to certain limitations. This right, an extension of the so-called general personality right, was coined in the landmark *Census Act* decision of 1983, a decision that heavily influenced the jurisprudential and legislative climate in the following decades. See Kaiser 2010 (6) No 3 3 *EuConst* 504-505.

854 Ibid.

855 Confidentiality on the other hand, is a set of rules that govern the use of information collected by institutions or individuals from persons who maintain relationships with them and the conditions under which such information can be shared. Secrecy relies on an informal and usually unenforceable agreement on the part of those who are party to some information, not to share it with others.

856 See n 850 at 475. See also n 851 at 7.

or the administration of health care programmes. They may also be required, oftentimes by means of extant legislation or regulations, to disclose their personal information because without such disclosure, the benefit or service required will not be given to them. Usually the personal information collected is disclosed on the understanding that it would be used for the specified purpose for which it was given. Experience now shows that very often, personal information disclosed for one purpose, is used for other purposes as well.

3.2 The value of freedom of information

Some of the benefits of having a freedom of information law have already been highlighted earlier.[857] One of the strongest arguments for freedom of information is that a freedom of information law is a very effective tool to empower the public to hold governments, public servants and even the private sector accountable. When information held by governments becomes easily accessible to the people, they can see for themselves that the government is doing what it says it is doing and more importantly, take steps to make the government accountable for what it is not doing right. Access to information also facilitates economic development when investors, local and foreign, are able to easily access information about the regulatory and legislative environment of a country they plan to invest in. Access to information about investment incentives and guidelines on how to obtain relevant government approvals and licences will enable a prospective investor to quickly determine whether to invest or not.

A fundamental principle of the concept of freedom of information is that every citizen should have the right to access information held by the government for the reasons given above. On the other hand, the core element of information privacy is that individuals should, in general terms, have control over access to their personal information by third parties. This is of course the ideal position or expectation, which is subject to exceptions. These exceptions have been found to be reasonably necessary in many developed and developing countries and they facilitate the exercise of the right to freedom of information. However, the enactment of freedom of information laws across the world has not resolved the underlying tension

[857] See par 1.1 above.

between the concerns for greater openness which freedom of information laws engender, and the desire to protect personal information privacy.[858] One consequence of the tensions between information privacy and freedom of information is that securing one person's privacy may infringe on another person's freedom of information.

The right to freedom of information is an essential aspect of the right to freedom of expression and understandably so because in terms of the definition of freedom of expression, it is usually formulated as including a right to "receive" information.[859] In practical terms therefore, without access to information, other human rights such the right to private and family life cannot be effectively exercised. As the ability to express oneself and impart information is contingent on the ability to access information, the rights to freedom of expression and privacy must of necessity, involve the protection and exercise of the fundamental human right to access to information.

3.3 Freedom of information v information privacy in Nigeria

It was noted at the beginning of this chapter that technological advances in the collection of information and the new business models for trading in such collected information seriously threaten the whole notion of information privacy. This threat is further enhanced by the fact that trade in personal information as a commodity provides incentives today for even more egregious collection of personal information. The enactment of the Freedom of Information Act in 2011 in Nigeria further widens the scope of access to personal information kept by governments and some private entities providing public services. This widened scope of access is particularly beneficial to the practitioners of journalism who had been in the vanguard of the clamour for the Freedom of Information Act. Furthermore, under section 22 of the Nigerian Constitution, the press, radio, television and other agencies of the mass media "[s]hall at all times be free to uphold the fundamental objectives contained in this chapter [chapter 2 of the Constitution] and uphold the responsibility and

858 McCamus 1986 (3) *Gov Inf Q* 49.

859 For example, see s 39 of the Constitution of the Federal Republic of Nigeria, 1999.

accountability of the government to the people." This provision assigns to the press, the duty of upholding the responsibility and accountability of the government to the people. However, in carrying out that duty, the press does not have and cannot exercise any right or power over and above the right to freedom of expression enjoyed by every other citizen. Ordinarily, the right to information and the right to privacy are both invaluable human rights and in a normal society are complimentary one to the other. This is however not always the case.

Concern for the security of the state and the preservation of public peace has always been the motivation for adopting measures, either by legislative enactment or judicial interpretation, to regulate the activities of the press. Among these measures in Nigeria are the Official Secrets Act,[860] sections of the Criminal Code Act[861] and the Defamation and Offensive Publications Act.[862] Other laws establishing public institutions also provide secrecy clauses which insulate such institutions from public scrutiny.[863]

The culture of secrecy and the mechanisms used by governments to create such a culture, vary from country to country. These measures range from the enforcement of a strict Official Secrets Act, based as it were, on the presumption that all information is restricted unless the opposite is specifically declared, to threatening and even murdering journalists who report on governmental duplicity. These mechanisms have all been used in Nigeria in recent years to create an unfavourable climate for accessing information in the country. It is in this light that the mass media, civil society groups and non-governmental organizations demanded a freedom of information law that will guarantee the right to seek and impart information. The press continues to clamour for a specific constitutional guarantee of press freedom, not as an adjunct of the right to freedom of expression as presently is

860 1962, Laws of the Federation of Nigeria 1990.

861 Chapter 7 Criminal Code Act, Laws of the Federation of Nigeria 1990.

862 Laws of the Federation of Nigeria 1990.

863 See the following laws: s 22 Border Communities Development Agency (Establishment, Etc) Act, 2003; s 7 Customs and Excise Management Act, 2003; S 50 Criminal Code Act; s 165-170 Evidence Act, 1945; S 31 Fire Service Act, 1990; s 10(2) Public Complaints Commission Act; s 8 Statistics Act, 1957.

the case.[864] Conflicts between the right to privacy and freedom of information usually arise where journalists or book publishers or authors, publish private information, usually without the consent of the person the information points to. The common justification for such publications is that the information published is a matter of public interest. It is left to the courts to determine whether such claims of public interest are justified by balancing the interests of information privacy against that of access to information.

3.4 Striking the right balance between the right to information privacy and the right to freedom of information

It is now settled, judging from provisions in national[865] and international legal documents such as Article 19 of the *ICCPR* on the right to freedom of expression, that it includes "freedom to seek, receive and impart information and ideas of all kinds". The right to seek information is of particular importance to the press; it is currently being articulated in various Freedom of Information laws across the world. The right of the press to seek and acquire information is justified on the ground that it is desirable to have an informed electorate which is able to assess the wisdom of governmental decisions. However, the freedom to seek and receive information under Article 19 and similar provisions guaranteeing freedom of expression as discussed above, impose no duty on any person to disclose information that he is reluctant to disclose. It does not provide a person with a right to extract information from an unwilling source.[866] Rather, it is a freedom from interference by the state or its agents.[867]

---

[864] In Innocent *Adikwu v Federal House of Representatives* 3 NCLR 394 (1982), the applicants, who were journalists, had been summoned by a committee of the of the House of Representatives in respect of a publication carried in the Sunday Punch newspaper of 5 April 1981. They applied under the Fundamental Rights (Enforcement Procedure) Rules 1979 to enforce their fundamental rights under section 36 of the 1979 Constitution. In granting their application, the court held that, "[t]he purpose of s 36 of the 1979 Constitution is not to erect the press into a privileged institution, but it is to protect all persons (including the press) to write and to print as they will and gather news for such publication without interference." (Per Balogun J at 417).

[865] See s 39(1) Constitution of the Federal Republic of Nigeria 1999.

[866] Barendt *Freedom of Speech* chapter III.5.

[867] Art 10 ECHR.

As was noted in the previous chapter, and in the particular context of the predominantly communal nature of African/ Nigerian societies, the desire to keep something private is often perceived as a desire to "hide" something. This mentality has been carried over into the practice of journalism. Matters that should otherwise remain private become the stuff of which many "news" headlines are made of. This is particularly so when the so-called "news" item concerns a celebrity. It is no secret that the practice of journalism in the enjoyment of the right to freedom of the press, has on many occasions breached privacy rights. The desire for protection from unwanted publicity frequently appears to conflict with the right to freedom of expression and of the press.

Given the fact that freedom of expression, a corollary of the freedom of information, is capable of violating privacy rights, it becomes necessary to strike a fair balance between the two sets of rights. In *A v B Plc,*[868] the need to strike such a balance between the requirements of the privacy right guaranteed under Article 8 of the *European Convention on Human Rights* (ECHR) and the guarantee of freedom of expression under Article 10 thereof, was highlighted. Lord Woolf noted:

> There is a tension between the two articles which requires the court to hold the balance between the conflicting interests they are designed to protect. This is not an easy task but it can be achieved by the courts if, when holding the balance, they attach proper weight to the important rights both articles are designed to protect. Each article is qualified expressly in a way which allows the interests under the other article to be taken into account.[869]

The traditional approach, in striking a balance between the two competing interests, is to use either privacy or freedom of expression as the starting point and then make allowances for the other.[870] If the starting point is the right to privacy, disclosure of

---

868 (2003) QB 195.

869 Ibid par 6.

870 See the American case of *National Archives and Records Administration v Favish et al* 124 S Ct 1570 (2004). The Respondent in this appeal, Favish, was sceptical about five Government investigations' conclusions that Vincent Foster, Jr, deputy counsel to President Clinton, committed suicide and filed a Freedom of Information Act (FOIA) request for, among other things, 10 death-scene photographs of Foster's body. The Office of Independent Counsel (OIC) refused the request, invoking FOIA Exemption

private facts would be weighed against public interest in disclosure. One of the most significant justifications for intrusion into the private sphere of a person's life by the press for example, is that of public interest. The justification usually proceeds on the assumption that because some members of the public will be interested in the details of a person's, particularly a celebrity's, lifestyle therefore such publication is in the public interest.

This fallacy was exposed in the Australian case of *Chappell v TCN Channel Nine*.[871] The claimant in the case was a well-known cricketer who sought an interlocutory injunction to restrain the broadcast of imputations concerning misconduct in his private life. In granting the injunction, Justice Hunt rejected the argument of the defendant that the private life of a public figure is always the subject of legitimate public interest. He held that the private conduct of a public figure was in the public interest only if either the public figure makes his private activity a matter of public interest himself, or when the private activity has some bearing on his capacity to perform his public duties.

While Lord Woolf, in the *A v B* case above, agreed that, concerning trivial facts, "... [i]n many of these situations it would be overstating the position to say that there is a public interest in the information being published..." he added however,

> [i]t would be more accurate to say that the public have an understandable

---

7(C), which excuses from disclosure "records or information compiled for law enforcement purposes" if their production "could reasonably be expected to constitute an unwarranted invasion of personal privacy" 5 USC § 552(b)(7)(C). On appeal to the US Supreme Court, the Court held that Congress intended to permit family members to assert their own privacy rights against public intrusions long deemed impermissible under the common law and cultural traditions. It further held that the exemption protects a statutory privacy right that goes beyond the common law and the Constitution. As a general rule, citizens seeking documents subject to FOIA disclosure are not required to explain why they seek the information. However, when Exemption 7(C)'s privacy concerns are present, the requester must show that public interest sought to be advanced is a significant one, an interest more specific than having the information for its own sake, and that the information is likely to advance that interest. Thus, where there is a privacy interest protected by Exemption 7(C) and the public interest asserted is to show that responsible officials acted negligently or otherwise improperly in performing their duties, the requester must produce evidence that would warrant a belief by a reasonable person that the alleged Government impropriety might have occurred. It is only when the FOIA requester has produced evidence sufficient to warrant a belief by a reasonable person that the alleged government impropriety might have occurred, will there be a counterweight on the FOIA scale for a court to balance against the cognizable privacy interests in the requested documents. The Court held that Favish did not produce sufficient evidence to put that balance into play. See also the English case of *A v B Plc* (2003) QB 195 where the question of balancing the interests in information access and privacy was considered.

871 (1988) 14 *NSWLR* 153.

> and so legitimate interest in being told the information… The courts must not ignore the fact that if newspapers do not publish information which the public are interested in, there will be fewer newspapers published, which will not be in the public interest." [872]

The latter part of Lord Woolf's argument seems to suggest that anything and indeed, everything should be published by the press in the public interest so long as it is said to be of interest to the public. With all due respect to the Lord Chief Justice, it is debatable whether every matter that is of interest to the public is necessarily also in the public interest. If that were the case, the common law tort of defamation, the equitable remedy of breach of confidence and the Constitutional right to privacy would be rendered nugatory.

3.5 Conclusion

Various states use national security and concerns for public peace and order as justification for interference with the rights to seek, express or control access to information. These interferences are usually by way of legislative enactments and judicial interpretations that limit the enjoyment of the rights of information, expression and privacy.

There is therefore an underlying tension between the need to protect the rights of individual citizens and the need to benefit the community as a whole. Nowhere is this tension more acute than in assessing the balance that must be struck between the natural desire of an individual to protect his or her privacy and the need of the community to obtain information to assist in making good policy decisions for the benefit of the community as a whole. This underlying tension also manifests itself when the desire for privacy is set against the need for freedom of expression to be as unfettered as possible and for information to be available within the community so that members thereof can make informed decisions. The challenge of reconciling the right to personal privacy and the right to access information plays out most clearly in cases which involve a dispute about the definition of "personal information".

---

[872] See n 868.

Resolving the tension between the two rights requires a balancing act by the judiciary. It is however not wise to treat privacy and freedom of information as mutually exclusive. Both rights are of equal importance in a free society; the right to information privacy would not impinge on the right to freedom of information. On the contrary, it would enable individuals exercise the right to free speech in a protected and more congenial environment. Priscilla Regan, for example, notes that one aspect of the social value of privacy is that it sets boundaries that the state, in its exercise of power, should not transgress in order to preserve, freedom of speech and association within a democratic political system.[873] The concern, as advocates of privacy protection are careful to point out, is that an erosion of privacy dilutes important shared values within a free and democratic state. Privacy constitutes a society's common attempt to promote rules of behaviour, accountability, decorum, and civility.[874]

In practical terms however, the delicate job of balancing the two contending interests has in recent years been complicated by the introduction of technology into almost every aspect of our public and private lives. Not even developing countries like Nigeria are spared the onslaught of ubiquitous technology; they are moving gradually from a period when government records were kept on paper, to the age of computers and a host of new devices and forms of documentation such as digital files, the Internet and cloud computing. These new technologies have vastly multiplied the amount of data in the hands of government, private sector industries and even individuals. They have also created new problems of how to protect the privacy and security of the vast storehouses of information generated daily and at the same time, give access to them. These problems impact both the right to privacy and the right of access to information.

As noted in the Report by the Privacy Commissioner of Canada to Parliament for 2006-2007:

> Times have changed - so too has the privacy environment. Technology has created new and complex privacy issues. In 1982, the internet, global

873 Regan *Legislating Privacy: Technology, Social Values, and Public Policy* 221-30.

874 Post 1989 (77) No 5 *Cal L Rev* 968.

> positioning systems, radio frequency identification devices, cross-border outsourcing and data mining were novel ideas. Today, these technologies are commonplace and are the key issues keeping privacy advocates up at night. Another generation of technologies that carry privacy risks – brain scans and smart dust, for example – is just around the corner... The Privacy Act was not designed to address the era we now live in and it is not up to the job of protecting Canadians in this changed world. In fact, it has been desperately out of date for many years.[875]

The changing times also present another complication that affects the balancing of the interests in privacy and access to information - the frequent claims of national security by governments across the world. It is conceded that one of government's primary responsibilities is to protect its citizens and this responsibility sometimes involves claims of national security. In Nigeria for example, both the Constitution and the Freedom of Information Act recognise national security as a valid ground for the government to exempt information from disclosure or the enforcement of privacy right.[876] The concern, with regard to access to information, is the danger that claims of national security may unduly limit the openness and transparency needed in a democratic society. In respect of privacy, there is the danger that increased powers of surveillance given to law enforcement and national security agencies may unduly invade personal privacy.[877]

It is certain that the need to strike the right balance between the competing interests in information privacy and access to information will continue to engage the minds of policy makers, legislators and the judiciary in most democratic countries for the foreseeable future. How the balance will be achieved to the satisfaction of all parties is not altogether clear. However, the starting point is that all concerned in the balancing activity accept that the need to encourage free exchange of information in an Information Age should not lead to measures that lose sight of the equally compelling, need to protect the privacy of the information particularly when that information is classified as "personal data."

---

875 Privacy Commissioner of Canada *Annual Report to Parliament 2006-2007: Report on the Privacy Act* 7.

876 See s 11, 12 and 14 of the Freedom of Information Act, 2011; s 45 Constitution of the Federal Republic of Nigeria, 1999.

877 See n 834.

CHAPTER 6

INTERNATIONAL REGULATION OF TRANS-BORDER DATA FLOWS

1. THE INTERNATIONAL MARKET PLACE AND TRANS-BORDER DATA FLOWS

1.1 INTRODUCTION

A global telecommunications network of networks forms the communications backbone of the 21st century's world economy.[878] This network of networks, the Internet, led to the emergence of a borderless, international marketplace which operates across multiple borders and jurisdictions.

The increasing worldwide use of computer-driven communications has created a huge demand for, and an associated international trade in information goods and services involving the cross-border flows of personal data. For example, whenever prospective travellers apply for visas and work permits, or when business transactions, ordinary telephone conversations and data transmissions take place, there is a continual stream of personal information crossing borders globally.[879]

While the free movement of information in national and international economies is important and benefits all, the cross-border movements are coming into conflict with the right to privacy, since a significant portion of trans-border information exchanges consists of personal details. The evolution of trans-border data flow regulations and the emergence of a global regime of trans-border data flow and data protection

878 This is much like the railroads, steamships, telegraphs and postal systems that formed the transportation and communications infrastructure of the 19th and 20th century industrial economies. See Neogi and Cordell 2010 (15) No 2 *JIB&C* 1.

879 Regan 2003 (59) No 2 *J Soc Issues* 263.

regulations will be examined in the light of the interplay between globalization and trans-border data flows. In particular, the external influences and pressures that globalization, powered by information technologies, exerts on local policies thereby instigating changes in national policies will also be examined. While trans-border data flows are inherently international in nature, such flows can and do impact on national policies, thereby touching national interests.[880] The argument will be made that foreign and domestic policies have become so enmeshed in a globalizing world that the domestic policies, particularly of developing countries, are very often determined by external influences. One such external influence is foreign market power.[881] In combination with globalization, foreign market power gives economically strong states the leverage to influence and indeed, dictate some of the policy directions of weaker states. The reality many nations face in the 21st century is that much of their domestic policy is determined or influenced by what happens outside their borders and beyond their control.

2. TRANS-BORDER DATA FLOWS (TBDFs)

2.1 Introduction

The movement of information from one country to another has been going on for many years. These trans-border flows of information have been in the form of publications, telephonic and broadcast communications, text or images recorded in a variety of media.[882] What distinguishes the type of information flow under consideration from the general flow of information is that it is basically made up of data transmitted by electronic means from one country to another for processing and storage in foreign computer systems. However, the category of data that has catalysed legislation on the regulation of TBDF is personally identifiable data or

---

880 See Robinson 1983 *Telecommunications Policy* 271.

881 Economically strong states such as the U.S, the EU and Japan exercise a great deal of influence on the world economy by reason of their market power. Particular reference is made to Germany, France, U.K, Spain and Italy, as not all member states of the EU are economically strong. This power enables them to obstruct access to trade opportunities with their local markets. See Hirschman *National Power and the Structure of Foreign Trade* 13-17, for a description of how strong economic states exercise their power to interrupt commercial or financial relations with other countries.

882 Martyn 1986 (12) 4 *IFLA Journal* 318.

name-linked data.

According to Adriana Nugter,[883] "the extended possibilities to transmit information almost without reference to distance, time or volume has given rise to a spectacular growth in data flow through the use of the international telecommunication networks." A typical example of the cross-border flow of information can be seen in the case of a subsidiary in one country, gathering data and transmitting the data to its headquarters in another. The headquarters may receive, process and store data from more than one country.[884]

At various times, these flows of information have been subject to restrictions and regulations for economic, security and public policy reasons in both the receiving countries as well as the exporting countries of such information.[885] Because of the explosive growth in the electronic generation and storage of data of all kinds, there has been a corresponding growth in international data traffic. In recent years however, trans-border data flows have increasingly been seen as a major international policy issue.

2.2 Defining "trans-border data flows"

The term "trans-border data flow" (TBDF) was invented in the mid-1970s by the OECD secretariat which served the Computer Utilization Group (CUG), a unit under the Committee for Science and Technology Policy (CSTP). The term incorporates the collection, programming, processing and use of automated information for administrative and other purposes. In coming up with the term "trans-border data flow", the concern of the OECD was to address not only the advances in electronics and the advent of computer-based communications, but also, and quite crucially, concerns arising from the possible misuse of personal information transferred instantaneously across national borders. The latter concern, that is, whether the privacy of individuals may be jeopardized by the processing, storage and dissemination of personal details, continues to dominate the TBDF regulatory

883 Nugter Transborder *Flow within the EEC* 204.

884 Hoyle 1992 (8) No 4 *CLS Rev 166*.

885 Reidenberg 2000 (52) No 5 *Stan L Rev* 1315.

debate.

"Trans-border data flow" came into prominent use in the early 1980s in response to European privacy concerns.[886] Mowlana defines trans-border data flows as the transfer of digitally encoded units of information for processing, storage or retrieval across national boundaries.[887] According to him, to qualify as trans-border data flow, three technical processes must be involved: transmission, storage and processing. Traditional telephone and telegraph technology provides transmission, but offers neither storage nor processing. Storage of data opens convenient access to large data bases, and processing allows manipulation of data in various forms and orders. This definition, Mowlana maintains, excludes trans-border data flows resulting from media products, such as news broadcasts, television programming and conventional telecommunication services. He makes the point that trans-border data flows are normally of "a proprietary" nature, often based on contractual relationships between parties. Therefore, electronic media products which involve mass diffusion are not considered as part of trans-border data flow. TBDF is personally identifiable data or name-linked data. The key feature is that the information involved in TBDF either undergoes some type of data processing or is accessed across an international border.[888]

2.3 Emergence of TBDF discourse

The most frequently discussed trans-border data flow issue is information privacy. According to Rein Turn,[889] the catalyst for international discussion of the issue was the publication in 1972, of a Canadian study, "*Privacy and Computers: A Report of a Task Force*", which highlighted the fact that Canadian record keeping organizations shared personal data of Canadian citizens with U.S. institutions such as credit

886 See Longworth *Transborder Data Flow* [online].

887 See Mowlana *International Flow of Information: A Global Report and Analysis* 45.

888 Ibid. See also Guynes, Guynes and Thorn 1990 (6) No 3 ISEJ 27-32; Novotny 1980 (16) No 1 *Stan J Int'l L* 156; Hoyle 1992 (8) No 4 *C L S Rev* 166. Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Convention No 108/1981). See also *OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data* (1981).

889 Turn (ed) *Transborder Data Flows: Concerns in Privacy Protection and Free Flow of Information* 5-6.

bureaus, insurance companies, law enforcement agencies and regulatory agencies.[890] The Report also highlighted the concern that Canadian data stored in US databases may be unjustifiably withheld and be subject to a lower level of privacy protection in the US.[891] The release of the study heightened international consciousness about the problems of trans-border data flows and led to several unilateral attempts by governments to protect their databases.[892]

In 1978, the IBI, in conjunction with the United Nations Educational, Scientific and Cultural Organization (UNESCO), organized an Intergovernmental Conference on Strategy and Policies for Informatics (SPIN-I) which was held in Spain.[893] The conference recommended international action in examining the social, political, economic and legal implications of TBDFs and the formulation of international instruments for regulating trans-border data flows.[894] The use of transnational communications systems had resulted in increased levels of governmental intervention and control of trans-border flows of data in order to curb the risks of data privacy piracy or loss.[895]

Given the fact that multinational corporations control a very significant portion of cross-border data flows, they are able to secure advantages for themselves, thereby

---

890 Mhlaba 1995 (12) *GIQ* 354.

891 Ibid.

892 Ibid. In 1979, Brazil established centralised control over the purchase of computers by the national government and later extended control to computer purchases by private industry, and established a national information policy. The effect of the centralised computer processing policy was to effectively forbid Brazilians from using computers located outside of Brazil for their information processing if local Brazilian computers can accomplish the necessary processing. In 1980, Canada enacted the *Banks and Banking Law Revision Act,* 1980 requiring that all data produced by Canadian banks be processed in Canada, unless special exemptions are obtained. See Damon 1986 (10) *Fordham Int'l LJ* 265-266 n 12.

893 Pipe 1985 (1) No 4 *Telematics and Informatics* 411.

894 Id at 412.The efforts at the international level should concentrate on:

- Distinguishing between questions relating to the data flows themselves and those relating to the means of transmission;
- Defining the conditions of compatibility between the principle of the free flow of information and the necessary regulations;
- Considering the political, economic, social and legal dimensions of the problem of data flows without seeking to reduce them, in a single international instrument, to only one of such aspects;
- Taking into account the special circumstances of the different regions and the state of advancement of thinking in the various geographical zones. Advantage should be taken inter alia of the work already done by the EEC, the Council of Europe and the OECD.

895 Samiee 1984 (15) *J Int Bus Stud* 141.

limiting the access that states and/or domestic industries have to trans-border data flows.[896] Concerned about the consequences of control of trans-border data flows by multinational corporations, many states, particularly developing countries, began to call for the regulation of data-processing by multinational corporations.[897] The regulation of data processing by multinational corporations became the catalyst for international regulation of trans-border data flows.

As noted by Tongeren,[898] restraining corporate data flow activities is often discussed in conjunction with a state's efforts to protect the use and dissemination of data/information about its national economy. Moreover, for many countries legal measures dealing with trans-border flows of data affect national economies by promoting and protecting their domestic data processing industries.[899] Efforts by states to create international rules for the regulation of corporate data-processing activities are predicated on the notion that possessing data/information contributes to development, power and sovereignty.[900]

2.4 Major players in trans-border data flows

2.4.1 Governments

The most significant actors in trans-border data flows are the various national governments across the world.[901] They are the owners and heavy users of international computer communication systems. They operate and manage domestic communication networks that send and receive international data traffic. In most countries, communication services are state-owned and operated.[902] Data communi-

---

896 Jussawalla and Cheah 1983 (7) *Telecommunications Policy* 289.

897 See n 895 at 145-147.

898 Tongeren 1981 (10) *Intermedia* 42-43.

899 Fair 1987 (40) No 1 *ICG* 30.

900 Ibid.

901 See n 887 at 47.

902 Eg, the three major telecom service operators in China are either fully or majority government owned. They are China Mobile, formed in 2000; China Telecom, established in 1958, broken up in 1999 and reformed in 2002; China Railcom, established in 2000, is fully government owned. See US Dept of Commerce, International Trade Administration website [online]. This is not true of the United States of America where communication systems are owned and operated largely by private organizations.

cations are provided through the Post, Telegraph and Telephone (PTT) monopolies. In Nigeria, the Nigerian Telecommunications (NITEL) company was until recently the only operator of the country's internal and external telecommunications facilities.[903]

2.4.2 Inter-governmental organisations

Intergovernmental organisations such as the International Telecommunications Union (ITU) and the International Telecommunications Satellite Organization (INTELSAT) are also significant actors in trans-border data flows. Although the ITU is not a communications services provider, administrative conferences held under its sponsorship impact telecommunications activities across the world as they determine core practices such as the allocation of radio spectrum frequencies.[904] The organisation provides a forum for the regulation of data communication technologies and for debating and resolving conflicts relating to trans-border flow of data.[905] INTELSAT is a specialised agency of the United Nations, responsible for planning, coordinating functions and setting standards for international communication facilities ranging from telephone and telegraph to broadcasting and data communication.[906]

---

903 Today, Nigeria has two primary gateway operators, NITEL and Globacom and a variety of private telephone operators, including the South African communications giant, MTN, which is now the leading mobile phone service provider in the country. As at March 2012, the 3 leading GSM operators in Nigeria, MTN, Glo and Airtel had 42,184,470, 20,846,604, and 18,028,385 subscribers respectively. See NCC website [online].

904 See n 887.

905 Ibid.

906 Ibid.

2.4.3 Multinational corporations

Data transfers in areas like human resources, financial services, education and e-commerce are now an integral part of the global networked economy. Information-intensive industries such as banking, insurance, airlines, telecommunications, multinational businesses and news agencies are heavily dependent on the instantaneous availability and dissemination of data, including personal data, around the world. Advances in technology enable data to be transferred quickly and stored for as long as it is necessary to do so.

The need to transmit vital management information between parent organizations, manufacturing and trading firms and their subsidiaries operating in more than one country calls for reliable lines of data communication. Governments also rely on data links via satellite and cable for military, diplomatic and technical communication and decision-making.[907] The number of industries involved in cross-border transfers of vital information continues to grow.

American companies such as International Business Machines (IBM), Microsoft, American Express and many others are dominant in the development and operation of data processing hardware and networks. These companies maintain very influential positions in the social and economic development of much of the world.[908] The American domination of trans-border data flows across national boundaries for processing, storage and retrieval was partly responsible for the concerns and indeed protests from both developed and developing nations.[909] By 1981, the United States was responsible for 80% of worldwide transmission and processing of data.[910]

Other multinational corporations such as GlaxoSmithKline, Coca-Cola and Cadburys are key players in the flow of data across borders; they use operational data for

---

907 See n 887 at 45.

908 As noted by the United Nations Centre on Transnational Corporations, the manufacturers of the computer equipment that support trans-border data flows, the production of the accompanying software and the development of the technology that runs the whole system are almost entirely limited to the industrialised countries with majority of such companies located in the US. These American companies play the leading roles enabling TBDF. See United Nations Centre on Transnational Corporations *Transnational Corporations and Transborder Data Flows: A Technical Paper* 46.

909 Wilson and Al-Muhanna 1985 (22) No 4 *J Peace Res* 289.

910 Mowlana *Global Information and World Communication: New Frontiers in International Relations* 107.

managerial decisions and to co-ordinate their business functions in geographically diverse locations. Companies such as Shell, ExxonMobil and Chevron in the oil sector are also major users of the telecommunications networks for cross-border transfer of data. Multinational financial institutions such as Citigroup, Standard Chartered Bank, Western Union and many more rely on information representing transactional data arising from credits, debits and transfers of money. The bulk of these transactional data contain personally identifiable information relating to customers' dealings with these institutions. Apart from credit and debit data, other data that form part of the international flow of data through cyberspace are medical histories, criminal records, employment and travel reservations, as well as scientific and technical data.[911]

2.5. Challenges arising from trans-border data flows

The emergence of an Internet-based global economy poses important new challenges for governments everywhere. Globalisation has fostered the continued growth of multinational corporations and the proliferation of common technologies such as the Internet, wireless communications, etc. The recent emergence of international terrorism and the rise of trans-national crimes such as money laundering and Internet scams, are also forcing governments worldwide to review their policy frameworks on information sharing and privacy.

Issues surrounding trans-border data flows have been debated since the early 1970s. Most of the issues, then as now, revolve around the extra-territorial impact of emerging data protection law in Europe.[912] A good deal of the discussion, particularly from the American perspective, has focused on the perceived ulterior trade protectionist motivations behind these original policies. Commentators in Europe, on the other hand, have been concerned about the creation of "data havens" and the effect such havens would have on efforts to protect the privacy rights of European citizens.[913] They were also concerned that their own national sovereignty would be

911 Ibid.

912 Bennett *International Standard for the Protection of Personal Information* [online].

913 Ibid.

undermined if personal data were sent overseas for processing to escape the stricter regulations in force in Europe.

Writing in 1980, Rein Turn[914] identified five key concerns arising from increased trans-border flow of information. These concerns are:

- The possible erosion of the sovereignty of a country when large amounts of data about its economy, resources, citizens or government operations are transmitted abroad.[915]
- Increased vulnerability to disruption of access to these data and the lack of control over them can put a country in a position of significant dependency on other countries.
- The possible erosion of privacy protection available to individuals in their home countries when personal data about them are transmitted to countries where privacy protection laws are weaker or entirely absent. The possibility of foreign "data havens" arises.[916]
- The increased complexity and technical difficulties in assuring data security and maintaining accountability in networks that span several countries, employ different types of transmission technologies, are operated by different organizations, and are subject simultaneously to several sets of different laws and regulations.
- Potentially adverse effects on the development or continued existence of domestic data processing expertise and industry in those countries that utilize foreign data processing services on a large scale.[917]

Similarly, in 1983, the Australian Law Reform Commission published a Report[918] which identified four TBDF issues that highlighted a number of important and often conflicting considerations:

---

914 Turn *An Overview of Transborder Data Flow Issues* 3 [online].

915 See par 4 below for a discussion of the threats TBDFs pose to national security.

916 Par 3 below examines how TBDFs threaten the privacy of personal information.

917 See n 914.

918 Australian Law Reform Commission *Privacy Report*.

- The overall need for continuous and uninterrupted flows of information between nations;
- The understandable desire of countries to prevent transfers of information that pose a threat to their security, or which violate the rights of their citizens;
- The undoubted economic value attached to information and the need to protect trade in it by generally accepted standards of fair competition; and
- The requirement for safeguards in respect of the security of personal information to protect individuals against its misuse.[919]

Privacy concerns have long dominated the TBDF debate at the international level. Right from the beginning, several European countries passed laws limiting the sharing and use of personal information. These laws specified general principles of fair information practice and authorized national regulators to prohibit the export of personal information to countries that lacked sufficient privacy protection.[920] In recent times however, other wide ranging issues such as economic and sovereignty concerns have emerged.

Under the rubric of economics, some of the issues that engage the attention of policy makers include the question of what impacts TBDF will have on the balance of payments, employment and competitiveness of a country's service industries.[921] Other concerns relate to the international division of labour and whether increased TBDFs of computer-based services will result in significant productivity gains to the firms engaged in the data processing industry.[922] Sovereignty concerns encompassing national security, jurisdictional/legal issues, socio-cultural impacts and vulnerability issues have also engaged the attention of commentators.[923]

They are of particular relevance to the main theme of this thesis because they directly affect Nigeria's aspirations to become a valued member of the global

---

919 Ibid par 605.

920 Reidenberg 1992 (60) No 6 *Fordham L Rev* 137.

921 Knoppers 1984 (9) *J Technology Transfer* 3-8.

922 Ibid.

923 Ibid.

network economy. There is a gathering momentum towards the enactment of data protection regimes that meet the standard set by the EU; this momentum compels states with such regimes to place restrictions on trans-border data flows to countries without adequate protection of information privacy. Countries such as Nigeria, with a questionable level of information privacy protection, are more or less compelled to play catch up, if they are not to be left out of the global network. In addition to the threats to information privacy and national sovereignty, TBDFs also challenge a country's national security and socio-cultural interests. Of the concerns highlighted above, the threats of trans-border data flows to personal information privacy and national sovereignty have been the most contentious and they will be examined in more detail below.

3. TRANS-BORDER DATA FLOWS AS THREAT TO THE PRIVACY OF PERSONAL INFORMATION

3.1 Introduction

The first major issue to emerge from trans-border data flow activities was the need for protection of personal privacy. In addition to bringing about business efficiencies and conveniences for users, the increasing volume of global data flows has also elevated the risks to information privacy. It was also feared that the exponential increase in the number of informational transactions occasioned by computerization would multiply the amount of incorrect, out-of-date, or incomplete personal data that are stored and communicated.[924]

Moreover, the development of new technologies and business models for processing personal data has led to a greater direct involvement of individuals in the way that their data are transferred to other persons or companies, governments and across national borders. This is reflected in the continuing expansion of electronic commerce and online social networks that have made it possible for individuals to initiate and even control the trans-border transfer of their personal data to a much

924 Ibid.

greater extent than in the past. Christopher Kuner cites the example of online hotel reservation systems; in the 1970s when the OECD Guidelines were drafted, hotel reservation systems were already being used but access was restricted to the companies participating in them, whereas today individuals can personally make reservations via the Internet and thus input their personal data directly.[925]

Once personal data has been revealed or uploaded to the server of a business entity, the person revealing or uploading the data loses control over it. Such individuals do not know and cannot predict how their personal information will be used by those collecting them. There is also the possibility that the information may be used in a manner unexpected by the owner of the information. When that happens, it infringes one of the cardinal principles of information privacy protection, that personal information or data should not be used for purposes other than those for which the data subject agreed to by revealing his personal data.[926] These concerns have been particularly keen with regard to the increased collection of personal information, breach of information privacy, uneven or unavailable privacy protection in many countries,[927] as well as national security and law enforcement concerns.[928]

3.2 Increased collection of personal information

The continued growth in the size of information and communication networks' sophistication and capabilities have resulted in greater risk to customer's personal information privacy. Part of the risk relates to the ever increasing volumes of cross-border flows of personal information which are reaching broader geographical areas,

---

925 See Kuner *Regulation of Transborder Data Flows* 11 [online].

926 See the *OECD Privacy Principles* which are part of the *OECD Guidelines on the Protection of Privacy and Trans-border Data Flows of Data* (1980). Data matching and profiling for example, infringe the Use Limitation Principle because, in data matching for example, investigating data matching is conducted to identify and investigate apparent discrepancies, or what are referred to as "hits". The comparison process seeks to verify the one set by reference to the other set. According to the Law Reform Commission of Hong Kong, investigative data matching is widely regarded as highly intrusive to privacy interests, particularly when employed in large scale programmes. Individuals identified as "hits" may be subject to adverse decisions without notice, such as the termination of a pension. As accurate matching is dependent on a number of data quality variables, it is dangerous to make such decisions without some form of verification of the matching results. See The Law Reform Commission of Hong Kong (Privacy Sub-committee) *Reform of the Law Relating to Information Privacy: A Consultative Document* 140-142.

927 See par 6.6.1 below.

928 See par 4 below.

and involving an ever-greater multiplicity of actors. This is likely to increase the number and cost of privacy breaches borne by individuals and organizations with the risk of leading to a loss in individual user trust.

The widespread availability of consumer data gives businesses the incentives to misuse the collected personal data of their customers. As noted by the British Information Commissioner, there is a thriving market for personal information, a lot of which are surreptitiously acquired.[929] This increased risk is reflected in the growing number of data security breaches which are publicly reported. The Privacy Rights Clearinghouse[930] maintains an extensive catalogue of data breaches and estimates that about 90 million records have been compromised since the ChoicePoint incident.[931] However, given the fact that many organisations do not publicise their security breaches, the true scale of the problem may not be known. In addition to conventional methods of collecting personal information such as interviews, surveys, census, more subtle and sophisticated means of collection are now in use aided by ICTs. These include data mining, profiling, data matching, and etcetera.

3.2.1 Data mining

According to Ann Cavoukian[932], the commercial value of personal information for profiling, risk assessment, marketing and other purposes, is creating an irresistible craving on the part of organisations for more personal information, and for greater access to such data. She describes data mining as a set of automated techniques used in extracting buried or previously unknown pieces of information from large databases. Successful data mining makes it possible to unearth patterns and relationships, and then use this "new" information to make proactive knowledge-driven business decisions. Data mining then, "centres on the automated discovery of

929 Information Commissioner's Office (UK) *What price privacy now? 5.*

930 See the Privacy Rights Clearinghouse *Chronology of Data Breaches* [online].

931 On February 15 2005, identity thieves set up bogus customer accounts through which they applied for and unlawfully obtained from Choicepoint, an information brokerage company, personal data of 163,000 persons kept by Choicepoint. Similar data breaches are reported in a compilation maintained by the Privacy Rights Clearinghouse *Chronology of Data Breaches* [online].

932 Cavoukian *Data Mining: Staking a Claim on your Privacy* 4 [online].

new facts and relationships in data. The raw material is the business data, and the data mining algorithm is the excavator, sifting through the vast quantities of raw data looking for the valuable nuggets of business information."[933]

There are two main types of data mining; one is the "pattern-based mining" and the other is "subject-based mining". In pattern-based data mining, the data miner relies on a model of assumptions about the activities and underlying characteristics of culpable individuals or the indicators of terrorist or criminal plans. The miner then searches databases containing transactional and personal information for "hits" that indicate a match between the model and the patterns left by potential evidence of criminal or terrorist plans or by potentially culpable individuals. The aim of this approach is to identify terrorists who seek to blend into the host population and its economic and social structures.[934]
In contrast, "subject-based" data mining involves data searches that seek information about a particular subject already under suspicion based on information derived from traditional investigative means, whether that subject is represented by a name, a telephone number, or a bank account number.[935] Whether pattern-based or subject-based, data mining harms information privacy because it undermines the individual's control of the use of his personal information. Pattern-based mining in particular, is a more problematic type because, as noted by Dempsey and Flint, it conflicts with the constitutional presumption of innocence and the Fourth Amendment principle that the government must have individual suspicion before it can conduct a search."[936]

---

933 Ibid.

934 Rubinstein, Ronald and Schwartz 2008 (75) *U Chi L Rev* 262. See also Cate 2008 (43) *Harv CR-CLL Rev* 438. (Noting that American government agencies have for long used subject-based data mining searches.)

935 Dempsey and Flint 2004 (72) *Geo Wash L Rev* 1459.

936 Id at 1466-67. Pattern-based mining also poses the danger of false positives. Data analysis can lead to an innocent person being placed on a watch list, investigated, or detained. As noted by Mary DeRosa "Perhaps the most significant concern with data mining and automated data analysis is that the government might get it wrong and innocent people will be stigmatized as "terrorists" simply because they engaged in unusual patterns of behavior or have some innocent link to a suspected terrorist. A major challenge in the use of these techniques is addressing the possibility of bad data or imperfect search models that result in "false positives"." See DeRosa *Data Mining and Data Analysis for Counterterrorism* 15 [online].

3.2.2 Profiling

The growth of the Internet and electronic commerce has dramatically increased the amount of personal information that is collected about individuals by companies, especially the ones engaged in electronic commerce over the Internet. These companies monitor and collect information on what sites their potential customers visit, the time and length of these visits, search terms they enter and the purchases they make. When collected and combined with other data such as demographic data, these diffuse pieces of information create highly detailed profiles of net users.[937] Profiling is the compilation of information from various sources, to create a profile of a particular person. It involves the inference of a set of characteristics (typical behaviour) about a person or collective entity and the subsequent treatment of that person/entity or other persons/entities in the light of these characteristics.[938] The profile derived from the variety of sources is often used to market products to that person. According to Miller[939] one of the particular dangers of data profiling is the human tendency to assume that because information comes out of an automated system, it must be true. Rather, data profiles have a potential to magnify and reproduce human error.

3.2.3 Data matching

Technical advances in computers and telecommunications allow marketers to target sales at likely customers via personalised messages and products. Marketing companies use data matching to put together a composite picture of an individual's likes, purchase habits, credit behaviour, etc., to give a more complete picture of the individual. Data matching relies on the availability of large databases or other repositories of personal information.

There are two related but distinct methods of data matching: one is to compare a

---

[937] Privacy International *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Development* 60.

[938] See Bygrave *Data Protection Law: Approaching its Rational, Logic and Limits* 301; see also Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 9.

[939] Miller 1996 (1) *Communications Law* 146.

given individual's personal details in one computer database against two or more other databases to see whether a material fact is correct. The other is to perform a 'side-by-side' comparison of two or more large databases, to detect trends, anomalies, potential duplicates, etc.[940] Data matching is also used by governments to combat fraud, eliminate waste in public expenditures and political canvassing, for example by matching the electoral register against other data.[941]

3.2.4 Spam (Junk mail)

"Spam" is the term used to describe unsolicited email messages sent in large quantity to recipients with whom there is no pre-existing relationship that would legitimize such contact, usually for the purpose of advertising products and services.[942] Spamming undermines the privacy of the recipients of spam mails by encroaching on the recipients' expectations of privacy. One might reasonably expect the reading of his or her email to be a private activity, with no one else knowing whether the mail was read, when it was read, whether or not it was forwarded to a friend or associate, or what kind of computer or email client one used in reading the mail.

Spammers are now able to track the efficacy of their messages by inserting hidden codes that render HTML[943] spam mails. Hidden HTML tags allow spammers to know that a message was received and read, when it was read, whether it was forwarded and may reveal which e-mail client was used, in addition to other information such as geographic location, the user's Internet service provider, etc.[944] These new

---

940 UK Parliament *Fraud and Computer Data Matching* 1. See also Flaherty *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and The United States* 344.

941 Ibid.

942 See Thorson and Sedore *Spam and Personal Data Privacy* 4-5 [online]. The Internet Service Providers Association (ISPA) of South Africa, a non-profit body representing internet service providers in the country, defined spam as follows: "Spam, or unsolicited bulk email, is the posting of emails to large volumes of addresses advertising a service or product which the recipient seldom wants. Unlike conventional junk mail where the sender pays the cost of postage, recipients of spam pay the transmission costs, either in the form of Internet access fees and/or telephone call charges." See ISPA *Spam* [online].

943 Hypertext Markup Language is the programming language used for creating documents on the World Wide Web.

944 Solove, Rotenberg and Schwartz *Information Privacy Law* 693. Since 2005, spam or junk mail has been recognised as a potential threat to the full utilization of the Internet and e-mail. At the 2005 Geneva World Summit on the Information Society (WSIS), WSIS participants recognized that spam is a "significant and

capabilities built into junk mail certainly impinge on the data privacy of the individual in whose e-mail the hidden HTML codes are embedded. The fact that e-mail has become an extremely popular communication tool makes it a versatile vehicle for trans-border data flows. [945] It also highlights the extent of the threat to information privacy that TBDFs engender at the global level and therefore requires appropriate responses from various states. Some of the responses, it is safe to assume, would in some measure, impose restrictions on trans-border data flows.

3.2.5 Cookies

Cookies are bits of data stored on an individual's computer hard drive when he or she visits a particular web site. The stored cookie creates a built-in history of sites visited, material browsed and purchases made. They enable a visited website to keep a record of the browsing habits and preferences of users of the website. Such data can be used for marketing purposes by targeting an individual with ads that are customized to his or her tastes; for some, this may represent a convenience while to others, it may be an annoyance. However, it is the absence of control over the collection or the use of the information that constitutes a violation of privacy which can be harmful to individuals where such information is personally identifiable such as credit card numbers and passwords. In a report released in 2012 titled *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* The American Federal Trade Commission noted that "[i]n today's world of smart phones, smart grids, and smart cars, companies are collecting, storing, and sharing more information about consumers than ever before. Although companies use this information to innovate and deliver better products and services to consumers, they should not do so at the expense of consumer privacy."[946]

---

growing problem for users, networks and the Internet as a whole" (WSIS Declaration, par 37), and that to build confidence and security in the use of ICTs, there is a need to "take appropriate action at national and international levels" (WSIS Plan of Action, par C5, d). See WSIS Documents [online].

945 In 2002, Belgium opened a spam mailbox (boîte à spam) for three months, in which the unsolicited commercial e-mails spontaneously forwarded by Belgian Internet users were stored. At the end of the project, the Belgian Privacy Protection Commission released a study on "spam," which made a detailed assessment of the phenomenon of spam in Belgium. One of the key findings was the fact that the majority of the junk e-mails were sent from outside Belgium, in particular, from the United States. See International Telecommunication Union (ITU) *Survey on Anti-Spam Legislation Worldwide* 14.

946 FTC Report *Protecting Consumer Privacy* i [online]. The Commission agreed that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any

4. TRANS-BORDER DATA FLOWS AS THREAT TO NATIONAL SOVEREIGNTY AND SECURITY

4.1 Introduction: TBDF and the transformation of sovereignty

Globalisation, as evidenced by the continued growth of multinational corporations, the availability of technologies such as the Internet and wireless telecommunications, is forcing privacy and data protection concerns into the mainstream of governmental policy considerations. No nation, organisation or individual wants to relinquish control over an important and strategic commodity as information. Gotlieb *et al*[947] have argued that the territorial basis of national jurisdiction and therefore of regulatory law, is probably the most immediate source of frustration for a country wishing to exercise control over the storage and use of data about its citizens located beyond its own borders.

The European Union's *Directive* on data protection is the most ambitious and far-reaching data privacy initiative so far[948]; it has been instrumental in placing data protection concerns in the global arena.[949] However, the issues arising from the Union's attempts to protect the information privacy of its citizens, raise difficult questions about territorial jurisdiction and indeed, about how political and territorial sovereignty are defined in the digital age.[950] According to Kobrin,[951] they illustrate an emerging geographic incongruity between the reach and domain of the territorially defined "Westphalian"[952] state and the deep and dense network of transnational

---

privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the unexpected revelation of previously private information, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g., purchase history, employment history) to unauthorized third parties see Id 8.

947 Gotlieb, Dalfen and Katz 1974 (68) *AJIL* 247.

948 Salbu 2002 (35) *Vand J Transnat'l L* 656.

949 See par 6.6 below.

950 Ibid.

951 Kobrin *Trans-Atlantic Data Privacy Dispute* 2 [online].

952 Kobrin "Globalization, Transnational Corporations and the Future of Global Governance" 249. The "Westphalian" system is named after the Treaty of Westphalia which established the formal equality of

economi
c relations that constitute the early 21st century world economy. This deep and dense network of transnational economic relations is the product of both economic and political globalization.

The guiding principle behind the system of governance that dominates the geo-political arrangement of modern states is that of territorial sovereignty.[953] Sovereign states are the basic actors in the modern contemporary international system. They are territorial units with juridical independence, and are not formally subject to some external authority; they have de facto autonomy.[954] This means that today's territorially sovereign states claim absolute political authority within their respective fixed territories. However, the growth in both the extent and reach of international agreements, treaties, conventions and codes in recent years, has resulted in national sovereignty becoming questionable as a dominant concept.[955] This tendency is becoming more noticeable particularly in the modern commercial environment and with particular reference to the Internet and ICTs.

One important aspect of national sovereignty refers to a country's ability to influence

---

nation-states in Western Europe. It is used by scholars for the extended period in which the nation-state was the central object of analysis in international law and thus international relations.

953 According to Liu, "[i]t is a recognized principle of modern international law that every independent and sovereign State possesses absolute and exclusive jurisdiction over all persons and things within its own territorial limits." See Liu *Extraterritoriality: Its Rise and Its Decline* 17.

954 Krasner distinguishes four different meanings of sovereignty; the first one is interdependence sovereignty, which refers to the ability of states to control movements across their borders. Secondly, there is domestic sovereignty which refers to authority structures within states and the ability of these structures to effectively regulate behaviour. Thirdly, there is the Westphalian sovereignty which refers to the exclusion of external sources of authority both *de jure* and *de facto*. This means that the state has a monopoly within its own boundaries, over authoritative decision-making. At the international level it implies that states follow the rule of non-intervention in the internal affairs of others. The fourth meaning of sovereignty, international legal sovereignty, refers to mutual recognition. The basic rule of international legal sovereignty is that recognition is accorded to juridically independent territorial entities which are capable of entering into voluntary contractual agreements. See Krasner 2001 (22) *IPSR* 229-233.

955 For example, Pritchard and Mulligan argue that:

> [s]overeignty is … analytically useless, not because we believe the sovereign state has been superseded, but because it is impossible to say with any degree of accuracy where sovereignty lies in the first place or whether a sovereign state has ever actually existed. A secular conception of sovereignty is always already compromised by the plurality of sovereigns, by the necessity of the un-sovereign other to constitute the sovereign, by the sheer contingency of social power and by the social, political, economic, cultural and religious structures that enable and constrain the actions of the people that would be sovereigns. See Prichard and Mulligan *The Poverty of Sovereignty* 18 [online].

the direction of its political, economic and socio-cultural changes.[956] One of the ways a country exercises its national sovereignty is its ability to take decisions independently without the interference of another country. The accumulation and storage of data forms part of the decision-making process; how effective the process is depends very much on unrestricted access to massive amounts of data.[957] A county's sovereignty is impaired when vital information affecting its national decision-making is processed and stored in foreign databases.[958] This happens when, in the course of taking a decision, access to vital information stored in a foreign database is restricted.

The restriction may be due to a sudden interruption to critical data flow arising from computer breakdown, natural disaster, political pressure or an undeveloped capacity to apply the necessary technology.[959] For example, the transfer of data from Nigeria by MTN, a South African telecommunications company operating in Nigeria, to South African data banks for processing and storage means that, potentially at least, South Africans will have the means to influence the decisions by and about Nigerians that depend on the stored data. This could be by way of limiting access to the stored data, determining what data is accessible so as to influence the decision-making process or in extreme cases denying access to the data.[960]

Also, the transfer of sensitive data to countries with inadequate or no data protection codes or to "data havens", could expose a country to data thefts or foreign manipulation.[961] The risks associated with trans-border data flows and the warehousing of data in foreign databases, have prompted many countries to adopt policy measures aimed at regulating and in fact, restricting TBDFs.[962] The race to

---

956 Mowlana *Global Information and World Communication* 115.

957 Ibid.

958 Ibid.

959 See United Nations Centre on Transnational Corporations (UNCTC) *Transnational Corporations and* Transborder *Data Flows: An Overview* 28.

960 On the other hand, to the extent that Nigerians lack data about themselves — either because they lack the computer capacity needed to effectively use the data or because important parts of the data are withheld by the South African state – means that they will be unable to make informed decisions affecting their future. This also results in the erosion of Nigeria's national sovereignty.

961 See n 956.

962 A study by the Canadian government on the impact of trans-border data flows concluded that "the

regulate and in some cases, restrict trans-border data flows is not without controversy. As observed by Novotny,[963] the competition between the exclusive interests of information control and the inclusive interests of unrestricted transfer of information across national boundaries is responsible for the controversy.

4.2 The "Free Flow of Information" versus "Sovereignty over Information Flow" debate

The controversy between free flow of information and sovereignty over information flow was particularly highlighted by the arguments for and against a New World Information and Communications Order (NWICO).[964] Throughout much of the 1970s and 1980s, the debate about a NWICO raged in the United Nations, and particularly within the UNESCO. The NWICO proponents and opponents alike accepted the premise of a link between economic progress and the availability of information. The suggestion that an imbalance in information production and distribution was responsible for uneven world economic development polarized the debate between the liberal theorists and the socialist analysts.[965]

Essentially, the debate revolved around the contending concepts of information as commodity and information as social good, as well as upon the freedom of information as an individual versus a collective right. The socialist analysts argued that national cultures and sovereignty were threatened by the concentration of ownership and control of both the news media and their distribution channels in Western countries. The control by Western countries constituted a form of cultural dominance and diminution of the national sovereignty of other countries particularly underdeveloped countries.

To safeguard their national sovereignty, the socialist analysts and their home

---

government should act immediately to regulate trans-border data flows to ensure that we do not lose control of information vital to the maintenance of national sovereignty." See n 959 at 29.

963 Novotny 1980 (16) *Stan J Int'l L* 145.

964 See The MacBride Commission *Many Voices, One World: Towards a New, More Just, and More Efficient* World *Information and Communication Order* 34-44, for a rendition of the key issues, arguments and controversies surrounding the debate about a New World Information Order.

965 Ibid.

governments articulated principles, practices and policies that promoted controlled use, restricted access, conservation, denial and decreased transfers of information.[966] Liberal theorists on the other hand, saw information more as a commodity than a social good and therefore sought the free flow of information by advocating policies that would increase the sharing, use, and exchange of trans-border data flows.[967]

The tension between the competing principles of national sovereignty and the free flow of information is the result of conflicting international principles embodied in different instruments.[968] For example, Article 19 (1) of the *International Telecommunication Convention*,[969] grants to member states "the right to stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to their laws, to public order or to decency…" and "to cut off any other private telecommunications which may appear dangerous to the security of the state or contrary to its laws, to public order or to decency."[970]

Similarly, although member states agree to take measures that will ensure the "secrecy of international correspondence",[971] they however "reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their internal laws or the execution of international conventions to which they are parties."[972]

In contrast, international instruments such as the *Universal Declaration of Human Rights* (UHDR), *International Convention on Civil and Political Rights* (ICCPR), the OECD *Declaration on Trans-border Data Flows*, and other international instruments, establish a presumption in favour of unfettered speech and free information flow.[973] Article 14 of the *General Agreement on Trade in Services*

---

966 Ibid.

967 Ibid.

968 Drake *ICT Global Governance and the Public Interest* 6 [online].

969 *International Telecommunications Convention*, (1982).

970 Art 19(2).

971 Art 22(1).

972 Art 22(2)

973 See n 956.

(GATS), allows member signatories to adopt measures for the protection of the privacy of individuals and the protection of confidentiality.[974] The seemingly contradictory attitude to information flow by governments around the world is reflected in the tension between encouraging the bringing of information into a country and the interest in controlling the flow of such information. No state, however liberal, is completely indifferent to what kind of information comes into its boundaries. In the past, the deployment and operation of early telegraphic links in Europe accepted the then current perception of the concept of sovereignty.[975] Telegraphic links ended at the boundaries of each state; international messages were telegraphed to the last territorial outpost of one state, transcribed, and physically carried to the adjoining state, there to be retransmitted telegraphically.[976]

This respect for territorial sovereignty by technology did not last very long; today, international telecommunications lines and data flows are linked up across national borders. Nevertheless, states have remained wary of the implications of instantaneous trans-border flows of telecommunications data; they recognize the need to formulate general guiding principles.

4.3 Impact of TBDF and international trade on national sovereignty

Unregulated trans-border data flows can diminish a country's sovereignty, particularly in the context of international trade and liberalisation of international financial flows. International trade connects domestic markets to international markets; it is the key mechanism for moving goods, services and technology around the world.

Although international trade has been around from ancient times, it is in recent history that it emerged in its formal style of exchange of goods and services among nations. Trade and globalization are inseparable. According to Held *et al,*[977] trade

---

974 See *General Agreement on Tariffs and Trade*, Annex 1B: *General Agreement on Trade in Services* (GATS), Art 5.4 *Annex on Telecommunications*.

975 See n 947.

976 Ibid.

977 Held, Mcgraw, Goldblatt and Parraton *Global Transformations: Political, Economics and Culture* 149-150.

globalization involves more than the exchange of goods and services between diverse nations; it suggests the emergence of worldwide markets for traded goods and services. It in fact assumes a trading system wherein trade activities between two countries have the potential of affecting the rest of the countries in the international trading system.

Trade globalization implies therefore, the existence of a global market for goods and services which impact national economies in the sense that national production of goods and services are increasingly conditioned by global competitive forces. Thus, national economic activity is embedded within international networks of trade.[978] There is an extensive and intensive network of trading relations between almost all economies of the world, involving diverse goods and services.[979]

This extensive global market has been facilitated by the existence of world-wide transportation and communication infrastructures, as well as the adoption of trade liberalization policies and integration of production.[980] The increased intensity of international trade makes economies more sensitive to international fluctuations in the demand for and prices of goods and services. Not only do fluctuations in the international arena affect the domestic economy as a whole, major trends such as the adoption of data protection mechanisms at the international level, also affect domestic policies.[981]

Industrial and economic policies as well as domestic laws and regulations are increasingly subject to international scrutiny and interference. Trade globalization has diminished state autonomy and greatly influences domestic policy directions. The global regulation of trade by WTO and other multilateral bodies has transformed

978 Id at 151.

979 Id at 173.

980 Ibid.

981 In the past, states were able to use domestic trade protection policies to raise their revenues, protect domestic industries and manage their financial relations with other countries. This is no longer the case. By the closing decades of the last century, tariffs and quota restrictions imposed by international multilateral institutions such as GATT and the WTO, as well as economic costs and other institutional constraints have severely limited the autonomy of states to influence the protection and direction of their domestic economic systems.

the traditional notions of national sovereignty.

Contemporaneously with the growth of trade globalization, the world is experiencing increasing cross-border flows of financial and capital resources due largely to trade and financial liberalisation. The liberalisation of financial industries arising from the GATS[982] agreement has encouraged and facilitated the rapid growth of financial globalization and an upsurge in trans-border data flows. Concerns about the privacy and security of personal data culled from innumerable financial transactions around the world have given impetus to the search for global norms of privacy protection.

4.4 National security and law enforcement concerns

The Internet, e-mail and cell phones have changed the way people communicate with one another. The technological advancements represented by these technologies signify a revolution in the way most people around the world communicate today. However, with every advance in communications technology, there is a correlated advance in surveillance technology. Thus, the advances in communications technology have also catalysed a similar revolution in the way governments around the world investigate crime and protect national security.

Trans-border data flows have become a matter of general concern to the security and intelligence agencies of many governments. It is no longer news to say that the events of September 11, 2001, have had a dramatic effect on life and society not only in the United States but also in almost every part of the world. Governments across the world reacted to the terrorist attacks by introducing legislations, policies, and the formation of agencies that have affected their citizens' privacy, freedom of expression, and access to information. Not surprisingly, governmental reactions to the events of 9/11 were particularly swift and severe in the US; other countries have also been influenced by the terrorist attacks on the U.S in their legislative responses.

In the weeks and months following the attacks, governments around the world rushed to pass legislation aimed at preventing future acts of terrorism. The laws largely targeted the flow of information, particularly on the Internet. They also call

[982] World Trade Organisation General Agreement on Trade in Services (GATS) website [online].

for closer scrutiny of communications traffic so as to enable security agencies to more readily identify possible terrorist plans and stop potential attacks before they occur. As governments have moved to protect their citizens and enhance national and global security, the balance between national security and civil liberties has shifted in favour of national security. The trend today is towards secrecy and surveillance rather than transparency and anonymity.

Laws touching on national security have been passed in the United States, Canada, the European Union, the United Kingdom, China, Russia, and various African countries.[983] The revised national security policies of many countries such as the US, Canada and the UK, in the face of the war against terrorism, raise substantial concerns regarding trans-border information flows. For example, law enforcement and national security agencies in the US now have greater access to user information held by Internet service providers and have been empowered to spy on Internet users, thanks to the *Patriot Act*.[984] In the post-September 11th environment, not only are governments more keen to control information flow, there is also increased governmental cooperation and information sharing arising from the desire of governments' to conform to and participate in international agreements and policies.

As the 21st century continues to unfold, privacy issues will form part of the wider social and political dilemma about the role of public and private institutions in the use of various technologies. Tensions over individual privacy are becoming increasingly common in a range of contexts in modern life. The commercial value of

---

983 Hamilton *September 11* 2-3 [online].

984 Ibid. In the case of Africa, at the 35th Assembly of the Heads of State and Government of the Member States of the African Union (AU) held in Algiers on 14 July 1999, the 53 members of the Union adopted the *Convention on the Prevention and Combating of Terrorism.* In October 2001, Member States of the African Union adopted the Dakar Declaration against Terrorism, thereby reaffirming their unequivocal rejection of terrorism. In September 2002, an inter-governmental meeting held in Algeria adopted the African Union Plan of Action for the Prevention and Combating of Terrorism. See United Nations Office on Drugs and Crime (UNODC) *A Review of the Legal Regime against Terrorism in West and Central Africa* (2008) 1-5.

In Nigeria, the new *Terrorism (Prevention) Act*, 2011 provides measures for the prevention, prohibition and combating of acts of terrorism and the financing of terrorism in Nigeria It also paves the way for the effective implementation of the *Convention on the Prevention and Combating of Terrorism* as well as the Convention on the Suppression of the Financing of Terrorism, and prescribes penalties for the violation of its provisions. The Money Laundering (Prohibition) Act, 2011 repeals the Money Laundering (Prohibition) Act, 2004 and makes comprehensive provisions to ban the financing of terrorism and the laundering of the proceeds of crime or illegal acts. See Nigerian Financial Intelligence Unit [online].

personal information for marketing and other purposes is creating an irresistible craving on the part of organisations for more personal information, and for greater access to such data. Governments too are eager for more data on individuals to assist them in criminal justice and national security activities by the state. Information and communication technologies now make possible, levels of surveillance and information processing that once seemed unimaginable.

The imperatives of national security and law enforcement are wearing away traditional expectations of a right to privacy. The sophistication of modern technology now means that little can be forgotten or lost. Although most personal information is originally collected and processed for legitimate and appropriate reasons, the mere existence of this vast pool of personal information constitutes a covert invitation to misuse. This is a temptation that many employees find difficult to resist.[985] Personal information collected by organizations become natural targets for compromise usually because of the sensitive nature of such information (e.g., financial information, customer purchasing habits, preferences, etc.). A significant number of the compromises arise from mishandling by employees of the collecting agencies who have access to the valuable information, and abuse their access rights. These employees steal sensitive personal information from computers they have access to and sell them to others who misuse such information.[986] No doubt technology has a major impact on the gathering, storage, retrieval and dissemination of information, but its main ethical challenges relate to issues of accessibility and technological manipulation of information. These challenges impinge on the value of information privacy.

985 For example, Froomkin argues that if a copyright management system connects via the Internet to the content owner to ensure billing or even payment before access, then only the most sophisticated user will be able to determine how much information is being transmitted. See Froomkin 2000 (52) *SLR* 1489. See also Weller and Shaffer 2008 (26) *Association of Corporate Counsel Docket* 88.

986 See FBI *The Insider Threat* [online].

5. LEGAL AND JURISDICTIONAL ISSUES ARISING FROM TBDFs

5.1 Introduction: extra-territorial application of domestic laws

The Internet is the foremost channel of trans-border data flows. Because it provides businesses with an additional and usually faster means of communication with their customers, commercial activities are no longer confined to national or regional borders. For many businesses, access to national and international markets is available because the Internet transcends boundaries and provides links to areas that were once unreachable. This expansion of the marketplace beyond national borders carries with it increased risks of conflicts and litigation.

One of the consequences of globalization is that a country's interests are no longer contained exclusively within its territorial borders. As noted by Kobrin, "in an interconnected world it is increasingly likely that the legitimate decisions made by states will affect people and areas outside of a state's sovereign domain…"[987] This can readily be seen in the area of regulatory differences between nations when there is cross-border "spillover" from one national jurisdiction into other jurisdictions. Such spillover occurs when (1) the impact of the regulation is not (or cannot be) limited to the geographic territory of the originating jurisdiction, and (2) state capabilities and authority in other affected jurisdictions are constrained to the point where impacts cannot be mitigated.[988]

Many countries, particularly the advanced Western economies, find it increasingly necessary to assert their legal jurisdiction beyond their borders. Such extraterritorial assertion of legal authority may well interfere with the sovereignty of other countries.[989]

5.2 Territoriality

Territoriality refers to a world divided into clearly demarcated and mutually

---

987 Kobrin 2004 (30) *Rev Int'l Stud* 111 112.

988 Id at 111.

989 See Coughlan, Currie, Kindred and Scassa *Global Reach, Local Grasp* 5 [online].

exclusive geographic jurisdictions; it also implies a world where economic and political controls arise from control over territory.[990] According to Kobrin,[991] the principle of sovereign territoriality provides autonomy and ultimate law making and law enforcing authority to states within their geographic borders and over their citizens abroad. It is this idea of mutually exclusive geography that underlies the modern state system.[992]

Although in general terms, a country cannot exercise its legal authority outside its borders, yet so much of the country's economic life depends on the flow of information into and out of it. The regulation of data export/import implicates the laws where they originate and the laws of the receiving countries. Gotlieb *et al,* have suggested that the issues of trans-border communication should be viewed in the light of the "tension between the conflicting state interests in protecting, conserving and controlling information on the one hand, and of importing, exporting and exchanging ideas on the other - both in pursuit of state goals and in support of national policies."[993]

In the process of balancing the competing benefits of promoting and restricting the flow of information, the domestic regulation of trans-border data flows in one country may impinge on the rights of residents in other jurisdictions. For example, in 1995, the Bavarian Justice Ministry in Germany prosecuted a German subsidiary of an American company CompuServe, for carrying on-line discussions that violated German anti-pornography laws.[994]

The company, an Internet services provider, hosted discussion groups involving

---

990 Kobrin No 107 *Foreign Policy* (1997) 74-75.

991 Kobrin 2001 (32) *J Int Bus Stud* 691.

992 Ibid.

993 See n 947.

994 Nash January 15, 1996 *The New York Times* [online]. Another example is the French case concerning Yahoo!; the Internet portal enabled the auctioning of Nazi memorabilia. Yahoo! was ordered to prevent French nationals from accessing sections of its website that traded in Nazi artefacts. The challenges of identifying "French nationals" whilst online were simply too much for the company. In the end, Yahoo! prevented all users in all countries from accessing the auctions-site. See Akdeniz 2001 (3) *EBLR* 110-120 [online].

persons from around the globe, including the one based in Germany. In its initial response, CompuServe blocked access to the discussion groups in Germany. However, CompuServe's response to the Bavarian regulation had the effect of blocking access to these discussion groups for all CompuServe users worldwide. The consequence was that the Bavarian regulation interrupted the flow and availability of the discussion groups for CompuServe clients outside Germany.

5.3 Extraterritoriality and the regulation of TBDFs

It is a settled principle of international law that one state's exercise of sovereign power cannot infringe upon the sovereignty of another state or states. According to Kobrin,[995] the principle of sovereign territoriality provides autonomy and ultimate law making and law enforcing authority to states within their geographic borders and over their citizens abroad. Applying laws and regulations to non-citizens outside of one state's borders (extraterritoriality), violates the idea of mutually exclusive geography which underlies the modern state system. The extraterritorial application of national laws - that is, when one country imposes its laws on persons operating outside its territory, creates conflicts between jurisdictions. The question of extraterritoriality in relation to information privacy arises in respect of the EU Directive on privacy because of the provisions in Article 4(1)(a), (b) and (c) of the Directive.

A strict interpretation of these provisions points to a potential application of EU data protection laws to companies, persons or other entities engaged in the collection, processing, storage or transmission of information that are outside the EU but use EU-based equipment or service providers or to website owners with no servers in Europe but whose website is available to European Internet users. It follows therefore, that a Nigerian company, FirstBank Plc, for example, with a banking website available to Nigerians with Irish citizenship in Dublin, who have accounts with the bank in Nigeria but the bank has no office, equipment or staff in Ireland, is potentially subject to the Irish Data Protection Act in regard to the collection of personal information from its customers resident in Ireland. A legitimate question that arises is whether Article 4 of the *Directive* creates a wider jurisdiction for EU

[995] See n 991.

countries than the commonly recognised physical presence or conduct in the territory bases for prescriptive and adjudicatory jurisdiction.

5.3.1 Jurisdiction

Jurisdiction in the general sense is rather amorphous and therefore capable of more than one meaning depending on the circumstances under reference. Used in a strict legal sense, it is equally capable of various definitions. For example, it may mean the inherent or constitutional powers of the courts to hear and determine disputes. It may also mean the geographical area within which the courts can and do exercise their judicial powers. Jurisdiction is defined as "the power of the court to decide a matter in controversy and presupposes the existence of a duly constituted court with control over the subject matter and the parties."[996] In this sense, it is commonly known as territorial jurisdiction. Under international law, jurisdiction "reflects the basic principles of state sovereignty, equality of states and non-interference in domestic affairs."[997]

Historically, jurisdictional rules were developed to describe and balance the various interests of sovereigns to the conduct of persons or things as well as to other sovereigns.[998] As the volume and variety of cross-border interactions between nations continued to grow, extraterritorial application of national legal powers became inevitable. Extraterritoriality therefore refers to a state's ability to exert its power in ways that involve and affect people, places and things that are beyond its borders.[999]

According to Coughlan *et al*,[1000] the broad purposes of extraterritorial action by governments can be said to fall under three general headings:

- To control or affect the behaviour of individuals;

---

996 Black's *Law Dictionary*.

997 Shaw *International Law* 645.

998 Colangelo 2007 (48) *Harv Int'l L J* 129.

999 Coughlan, Currie, Kindred and Scassa *Global Reach, Local Grasp* 4 [online].

1000 Id at 10.

- To control or affect the behaviour of corporations; or
- To control or affect the behaviour of other states.

Although a great deal of extraterritorial activity takes place in the realm of competition law,[1001] there are growing instances of extraterritorial legislation by states in areas such as human rights, environmental impacts, international financial and securities regulation.[1002] The US has been at the forefront of the extraterritorial application of national laws, both as an advocate and user of the practice.[1003] This usage has occurred mainly in the area of competition/antitrust law, but also in its criminal, environmental, financial and securities, foreign sanctions and trade laws.

The arguments for and against the extraterritorial application of national laws have been succinctly highlighted in a submission by the Australian Chamber of Commerce and Industry (ACCI).[1004] According to the ACCI, supporters of extraterritorial application of national laws argue that:

- In an increasingly globalised marketplace, illegal/improper commercial conducts in one market often have adverse effects in another market across the border (spill-over effect). These spill-over effects are especially critical in globally integrated sectors such as banking, finance, insurance and securities, and in closely linked markets relying on competition and environmental laws. These spill-over effects, Post and Johnson declare, are "effects of conduct [that] extend beyond pre-established geographical boundaries—or 'spill over' into other jurisdictions…"[1005] Concern over international spill-over effects was recognized in 1980, when the OECD issued its Guidelines on the protection of

---

1001 Id at 12.

1002 Ibid. See also Wolf and Tobin "Extraterritorial Applicability of US Privacy Laws" Chp 28(1) [online]. The authors explain that some state-enacted privacy laws in the US have potential extraterritorial reach. Some of these laws apply to "any person or business that conducts business in [the State]" and require notice "to residents of [the State] whose information was, or was reasonably believed to have been acquired by an unauthorized person." According to the authors, the phrase "conducts business" means the laws apply to non-U.S. corporations who "conduct business" in the applicable State.

1003 See *United States v Verdugo-Urquidez* 494 U.S. 259, 281 (1990); *United States v Yousef* 327 F.3d 56 (2d Cir. 2003*); United States v Yunis* 924 F.2d 1086, 1091 (D.C. Cir. 1991).

1004 ACCI *Extraterritorial Application of National Law* 3 [online].

1005 See Post and Johnson 1996 (48) *Stan L Rev* 1378.

personal information.[1006] The Guidelines established principles for companies around the world to apply in the fair collection and use of personal information.

- When developed countries adopt vigorous policing of breaches of key economic laws (such as competition, finance and securities), other nations, in particular developing and transitional economies, will be encouraged to enact and/or raise the standards of their own laws in these areas.

On the contrary, critics and opponents[1007] of the extraterritorial application of national laws argue that it:

- Undermines the fundamental principle of international law, namely the respect between nations of the existence and integrity of national sovereignty, by allowing one state to interfere in the affairs of another state;
- Breaches the spirit of international comity, that is of co-operation between nations, resulting in conflicts between nations; and
- For business, it can result in unnecessarily complex and costly systems of overlapping and even inconsistent (and potentially unworkable) legal obligations especially for those operating across national borders.[1008]

Sometimes, measures are introduced by one state, to have extraterritorial reach by influencing the actions of other nations; the EU *Directive on Data Protection* is a good example of such a measure.[1009] It provides that EU member states must legislate so as to prevent the trans-border movement of data for processing abroad in a country that has not enacted legislation establishing adequate data protection norms. A pertinent question that arises is whether the *Directive* has any extraterritorial effect.

1006 Kuner *Regulation of Transborder Data Flows* 11 [online].

1007 See ICC *Extraterritoriality and Business* [online].

1008 Ibid at 3.

1009 See n 999.

6. THE EMERGING GLOBAL DATA PROTECTION REGIME

6.1. INTRODUCTION: THE EVOLUTION OF TRANS-BORDER DATA FLOW REGULATIONS

During the 1960s and early 1970s, the focus of many national computer policies in the United States and other Organisation for Economic Cooperation and Development (OECD) countries, was on the procurement, efficient operation and integration of computer mainframes and software for the processing of basic governmental, administrative or financial records.[1010] By the mid-1970s, the use of computers and software had spread into developing countries.[1011] In 1974, the United Nations established the Intergovernmental Bureau for Informatics (IBI) to aid developing countries in creating computer infrastructures and draw up policies on the use and priorities given to data processing services and equipment.[1012]

The global spread of computers and computer-generated data flows prompted a number of states and international organizations to examine the content of computer-generated data flows.[1013] Governments in various developed countries intensified legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Increased public awareness and interest in the risks and implications associated with the computerised processing of personal data prompted some European countries to enact statutes dealing with privacy protection issues arising from automated data processing (ADP).[1014] These laws specified general principles of fair information practice and authorized national regulators to prohibit the export of personal information to countries that lacked

---

[1010] See Fair 1987 (40) No 1 *ICG* 27.

[1011] Ibid.

[1012] Pipe 1985 (1) No 4 *Telematics and Informatics* 410-411.

[1013] The International Telecommunications Union (ITU) for example, has primarily been concerned with the technical aspects of computer technology proliferation; the ITU concerns itself with equipment and technological standardization.

[1014] The first laws that expressly protected information privacy were passed in Europe in the early 1970s beginning in Hesse, West Germany which passed its Datenschutzgesetz (Data Protection Act) in 1970. The term "Data Protection" soon came to be used in virtually all discussions of information privacy. Sweden was the first country to enact a national data protection legislation in 1973. See Bennett *Regulating Privacy* 77.

sufficient privacy protection.[1015]

6.2 Why regulate TBDFs?

The rapid advances in ICTs generally and computer technology in particular has heightened concerns about computer-based record-keeping because of the increasing capacities of these technologies to collect, process, store and distribute personal information locally or across international borders. Marsden[1016] refers to technology and globalization as two structural forces that are creating a dynamic information revolution in which the traditional notions of national law, nation-state, regulation and spatial parameters are being displaced by a new dynamic digital environment dictated by ICTs. The greatest medium through which personal and non-personal information is disseminated is indisputably, the Internet, or as some would call it, "cyberspace". Today, millions of people access the Internet on a daily basis and many use the medium for the purchase of goods, services, or information.

According to Marsden,[1017] "cyberspace" is mostly characterized by reference to the Internet; it is the virtual, non-physical, space between computer terminals across which most communication now flows. The telephone is now also a digital device which conveys information by the same technical means, as are the television and radio. Because the space is not "real" in a physical sense, it raises novel issues of regulation. Once it is accepted that this virtual space is a community of those employing it to communicate, that it is a marketplace of both ideas and digital products, and that it can be used for criminal activity and crime prevention, one begins to approach the view that cyberspace" is a territory.[1018]

This territory is international, indeed, transnational, because anyone can connect to anyone else who has access to cyberspace.1019 National policies and regulations

---

1015 See Reidenberg 1992 (60) No 6 *Fordham L Rev* 160-165.

1016 Marsden 2001 (2) *Det C L Mich St U L Rev* 360.

1017 Id at 355.

1018 Lessig 1996 (45) *Emory L J* 1.

1019 Ibid.

concerning TBDFs are inevitably affected by international policies and regulations because TBDFs cross national borders and are therefore international in scope.1020 However, the technological complexity and the increasing volume of data flows have rendered existing institutions, policies and regulations insufficient.[1021]

The concerns over TBDFs arise from the competition between two values: the values of sovereignty and the free flow of information.[1022] The debate about information privacy essentially revolves around the control of the flow of personal information in all stages of processing, i.e. acquisition, disclosure, and use.[1023]

The evolution of a new legal regime with particular rights and responsibilities relating to TBDFs is happening at a time when the opportunities for abuse of processed or stored data have increased considerably. The need for harmonized governing principles in the treatment of data crossing national boundaries has become compelling. The expansion of TBDFs has been greatly assisted by multinational corporations (MNCs) who have played the vital role of providing the hardware, software and computer infrastructure links.[1024]

As primary data users and processors, these corporations have established global computer/communications systems as a means of integrating affiliates, subsidiaries and markets in the efficient production and distribution of goods or services.[1025] As noted by Mowlana,[1026] these MNCs, empowered by a computerized global banking

---

[1020] Robinson 1983 (7) *Telecommunications Policy* 271.

[1021] Feldman 1983 (17) *The International Lawyer* 87-95.

[1022] See n 1005.

[1023] See Fried 1968 (77) *Yale L J* 475 at 482, saying "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves."; Miller *The Assault on Privacy: Computers, Data Banks, and Dossiers* 25, arguing that "[T]he basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him - a power that often is essential to maintaining social relationships and personal freedom."; Westin *Privacy and Freedom* 7, defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

[1024] Jussawalla and Cheah 1983 (7) *Telecommunications Policy* 289. See also Sauvant 1983 (37) *International Organization* 360-361.

[1025] Samiee 1984 (15) *J Int Bus Stud* 147.

[1026] See n 956 at 116.

system, are capable of bypassing national monetary policy. This makes the implementation of coherent financial policies by national governments very difficult.

6.3 Who controls the regulation of TBDFs?

Notwithstanding the current global approach to the regulation of TBDFs, states do not always share identical interests. The pattern of TBDFs between developed and developing countries differ; processed data flow to developing countries and raw data flow out to developed countries.[1027] Thus, the call for regulating TBDFs generally pits developed states - states that benefit most from TBDFs - against developing states.[1028]

Although electronic data flows across all national boundaries, it is not all nations that have developed or are developing new legal strategies for regulating conduct in cyberspace or conduct arising from the use of new technologies. It has therefore become imperative to adopt a global approach to resolving these problems. The emergence of the robust campaign for protection of personal data is a necessary concomitant of the pursuit of economic growth. One cardinal prerequisite of a free economy is the free flow of information. In 1997, the Federal Reserve Board of the US noted in its report on privacy to the American Congress, that "it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."[1029] The development of markets and international trade involves the cross-border flows of personal data between all the financial and social agents in the different countries that interact in a globalised world.

The issue that arises is how to control or regulate the flow of personal data across national boundaries in an orderly manner that would not put the data privacy rights of individuals to undue or unacceptable risks. In an ideal situation, a common benchmark on data privacy protection, with the necessary mechanism to achieve that

---

[1027] See n 1020 at 296.

[1028] Ibid.

[1029] Board of Governors *Availability of Consumer Identifying Information* 2 [online].

benchmark, will enable personal data to be collected, processed and used in a manner that would not raise conflicts or controversies. The situation today however, is far from ideal; there are inevitable variations within different jurisdictions in the areas of culture, economic development, legal and political systems. These variations make it difficult to formulate a universally acceptable benchmark of a common set of standards for implementing data privacy protection. Policy makers and regulators in different countries consider and pursue what they consider to be in the best interest of their countries; the result is the fragmented and sometimes overlapping regulations on data protection.[1030] It is certain that in the near term and even into the foreseeable future, TBDFs will continue to increase, powered by constantly improving technologies. With the increasing flows of data, there will be more pressure to protect personal information by means of a globally accepted template of policies and regulations.

Although, as noted by Lee Bygrave, "there does not exist a truly global convention or treaty dealing specifically with data privacy",[1031] there are regional treaties that have so far engendered international cooperation and harmonisation, albeit at regional levels. Examples of such regional data protection initiatives are the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,*[1032] the EU *Directives on Data Protection,*[1033] the APEC *Privacy Framework* (2005)*[1034]* and the Economic Community of West African States (ECOWAS) *Supplementary Act on Personal Data Protection within ECOWAS.*[1035]

[1030] Given the fact that there are divergent interests that drive the regulatory objectives of different countries, it is perhaps understandable why the level of harmonisation of the body of laws regulating TBDFs and the data protection issues arising therefrom is weak. However, it may be argued that there is some exception in the case of the US and the EU. These two jurisdictions are in fact the two foremost examples of cooperation in the area of data protection issues relating to TBDFs, because of the Safe Harbor agreement between them. The agreement allows US companies and organisations to comply with EU data protection regulations by giving them the choice to opt in to the regulations contained in the agreement, their compliance thereof being certified by the US government.

[1031] Bygrave 2004 (47) *Sc St L* 333.

[1032] ETS No 108 (1981). See also *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108) regarding supervisory authorities and trans-border data flows.

[1033] See par 6.6 below.

[1034] The APEC *Privacy Framework* (2005).

[1035] ECOWAS *Supplementary Act A/SA.1/01/10 on the Protection of Personal Data within ECOWAS Region of*

Regardless of their success at the regional level, data protection laws, as represented by the various regional and national laws, do not as yet constitute a field of law where "there has already been extensive State practice, precedent and doctrine".[1036] In the light of its statutory mandate, the International Law Commission (ILC) of the United Nations has noted that data protection is an area "in which State practice is not yet extensive or fully developed"[1037] to require codification.[1038] For this reason, it is not likely that an international covenant on data protection will emanate from the ILC any time soon.

It is suggested therefore that a regional approach to data protection be adopted for now until such time that all the regional data protection regimes, through implementation and enforcement, are able to present extensive state practice, precedent and doctrine sufficient to compel the ILC to undertake an international codification of data protection law under the aegis of the United Nations.[1039]

6.4 An international legal framework for regulation of TBDFs

The threats posed by TBDFs to personal information privacy and national sovereignty have prompted governments and their policy makers around the world, to adopt protectionist policies and/or laws aimed at regulating trans-border data flows. From an economic point of view, an efficient international information flow, together with international trade and investment, permit the optimal utilization of

---

2010.

1036 See United Nations General Assembly *Statute of the International Law Commission*, art 15.

1037 See United Nations General Assembly *Report of the International Law Commission* (58th Session) (Annex D), par 12 at 499.

1038 Wood *Statute of the International Law Commission* [online]. The main objective of the International Law Commission is the promotion of the progressive development of international law and its codification. Article 15 thereof defines "progressive development" as "the preparation of draft conventions on subjects which have not yet been regulated by international law or in regard to which the law has not yet been sufficiently developed in the practice of States." "Codification" is "the more precise formulation and systematization of rules of international law in fields where there already has been extensive State practice, precedent and doctrine."

1039 In 2005, Data Protection and Privacy Commissioners adopted the Montreux Declaration on the *Protection of Personal Data in a Globalised World: A Universal Right Respecting Diversity* [online], at their 27th International Conference held in September 2005, in Montreux, in which they called on the United Nations to draw up an internationally binding data protection convention.

global resources and thereby promote the exchange of data necessary for further innovation. For the international business community, there is need for unrestricted flow of business information because of the vital importance of the efficient exchange of information in the development and growth of modern international trade and production. Businesses need to communicate freely within and outside their corporate structures.[1040]

The need for an international legal framework that would constitute the basis for free international information flows has become compelling. Under such a framework, businesses can access and utilize national and international communications facilities on a fair, competitive and non-discriminatory basis. Many countries have, over the past decades, developed laws for the protection of privacy. These laws are as diverse in character as the different countries that enacted them. Many other countries are still in the process of developing their own regimes. The disparities in legislation may create obstacles to the free flow of information between countries. The legal requirements for various countries are different and do constitute a source of economic and organizational problems for companies engaged in international business activities. Different national provisions could therefore lead to restriction or prohibition of international flow of information.[1041]

[1040] For example, the Vice President of the American Express Company described the importance of TBDF to her organisation in the following terms:

> American Express, like other multinational corporations and especially service sector corporations, relies on automated, reliable and cost-effective global communication networks for the majority of its international operations. We have data processing centres around the world - including Brighton, Hong Kong, Singapore and Bahrain - all of which process data from, and disseminate data to, many different countries. Our card business depends on global communications networks… If open access were impaired American Express would encounter difficulties in providing a full service to its card members and be forced to decentralise at considerable cost. Communications are also essential for other internal operations; personnel records, in-house communication lines, internal budgetary procedures - all depend on our ability to transmit and store information within and across international boundaries.

See Savage and Edwards 1986 (35) *Int'l & Comp L Q* 713.

[1041] Citigroup, the multi-national American banking and financial corporation, in comments submitted to the European Commission on the review of the EU *Data Protection Directive*, noted that there are still significant differences in how member states of the EU approach privacy and data protection. This can be seen in the diversity of local laws implementing the *Directive* in member states. This is in addition to the variety of laws and approaches to the protection of privacy in countries outside the EU. The effect, the comment noted, is a lack of certainty and level playing field for companies operating in a pan-European or global environment. The result is that "businesses are required to take expensive legal advice and provide different services in each Member State, or to abandon plans altogether in the face of different laws."
See Citigroup *Review of the EU Data Protection Directive* [online].

Some nations have already gone very far in making necessary adjustments in their legal systems to address the unique features of modern technologies and the challenges they pose to privacy. Others have not, while some are perhaps beginning to do so. Existing laws governing communication and storage of information in many countries are inadequate or outdated, because they do not contemplate the use of modern technology and electronic commerce. A long-drawn out approach, nation by nation, to reformation in legal regulatory frameworks will inevitably give rise to tensions between nations and unduly hinder international trade. To minimize the conflicts therefore, nations seeking to derive benefits from the trans-border flow of information, must address the conflicts on a global platform.

6.5 International harmonization of data protection laws

Although the challenge of protecting personal data is almost universal, countries have developed different legal responses at different rates. Notwithstanding differences in national regulations across the world, the regulation of collection, processing and storage of personal information have in recent years tended to follow the principles outlined in the Code of Fair Information Practices.[1042]

Fair Information Practices (FIPs) are a set of principles and practices that prescribe how an information-based society may undertake information handling, storage, management, and flows so that fairness, privacy, and security is maintained in a

[1042] Fair Information Practices were initially proposed and outlined by a U.S. government advisory committee in a 1973 report. Elliot Richardson, Secretary of the Department of Health, Education and Welfare, established the committee in response to growing use of automated data systems containing information about individuals. The report, *Records, Computers and the Rights of Citizens*, was issued by the Secretary's Advisory Committee on Automated Personal Data Systems. See Gellman *Fair Information Practices* 1 [online]. These principles are:

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about himself.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

rapidly evolving global technology environment.[1043] FIPs are "the building blocks of modern information privacy law."[1044] According to Schwartz, FIPs are "centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight."[1045] They have played a significant role not only in framing privacy laws in the United States, but in the development of privacy laws around the world and in the development of important international guidelines for privacy protection.[1046]

The Code of Fair Information Practices formulated by the committee set up by the then American Secretary for Health, Education and Welfare in 1973,[1047] formed the basis for the Privacy Act, which the American Congress passed in 1974.[1048] The Act created a Privacy Protection Study Commission to examine a wide range of privacy issues in greater detail.[1049] The report[1050] of the Commission highlighted three fundamental objectives for any data protection system, and a number of specific recommendations for how those objectives might be achieved. The objectives are:

- To create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return (to minimize intrusiveness).[1051]
- To open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it (to maximize fairness).[1052]

1043 Dixon *Introduction to Fair Information Practices* [online].

1044 Schwartz 1999 (52) *Vand L Rev* 1607.

1045 Id at 1614.

1046 See Flaherty D *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* 306; See also Rotenberg 2001 (1) *Stan Tech L Rev* 6.

1047 See n 1042.

1048 Cate "The Failure of Fair Information Practice Principles" 3 [online].

1049 Ibid.

1050 The Privacy Protection Study Commission *Personal Privacy in an Information Society* [online].

1051 Id at 14.

1052 Id at 14-15.

- To create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual (to create legitimate, enforceable expectations of confidentiality).[1053]

The Code of Fair Information Practices and the report of the Privacy Protection Study Commission played a significant role in the development of the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* by the Organization for Economic Cooperation and Development (OECD) in 1980.[1054] The *Guidelines* identified eight principles to "harmonise national privacy legislation and, while upholding such human rights . . . at the same time prevent interruptions in international flows of data."[1055]

A number of international organisations have taken leading positions in the drive to

---

[1053] Id at 15.

[1054] Australian Chamber of Commerce and Industry *The Extraterritorial Application of National Laws: An Unwarranted Burden for International Business* 2.

[1055] See the preface to the Guidelines. The eight principles of the Guidelines are:

1. Collection Limitation Principle: 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.
2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law.
5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. 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.
7. Individual Participation Principle: 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 within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs(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.
8. Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

fashion out a new global regime of rules and regulations to address the issues affecting, and likely to hinder TBDFs in particular, and international trade generally. Efforts have been, and are being made at international level, to achieve a harmonious body of laws and rules for regulating TBDFs.

The impetus for these efforts is the recognition that privacy is an important trade issue; data privacy concerns can create a barrier to international trade.[1056] It is for this reason that the *General Agreement on Trade in Services* (GATS),[1057] for example, clearly states that the Agreement does not prevent member states from adopting measures "necessary to secure compliance with laws or regulations ... relating to ... (ii) the protection of the privacy of individuals in relation to the processing dissemination of personal data ..."[1058] International efforts to reduce the national discrepancies and to harmonize regulations in respect of trans-border data flows and information privacy have been undertaken in international organizations like the Council of Europe, the OECD, the EU, the United Nations, etcetera. Among the significant international initiatives taken so far to address the issues surrounding TBDFs, the following must be mentioned:

[1056] This fact is well recognized in the preamble of the EU *Directive 95/46/EC*; thus, realising the need to promote trade liberalization within the European Union and remove the threats to it as a result of uneven data protection laws in member states, the *Directive*'s preamble provides:

> (7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level...
>
> (8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States..."
>
> (9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy...

[1057] World Trade Organisation *General Agreement on Trade in Services* (GATS) (1995).

[1058] Art 14.

6.5.1 The OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data

In 1980 the Organisation for Economic Cooperation and Development (OECD), released the *Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data*.[1059] This was perhaps the most significant attempt at international harmonisation of information privacy protection at the time. The Guidelines were intended to provide a common framework for national privacy laws, in order to ensure that privacy concerns do not impose a barrier to international trade.

The OECD Guidelines are voluntary and were intended to provide an interim standard without creating unjustified obstacles to trans-border data flow. They establish technologically neutral principles for the collection, retention and use of personal information. The OECD's work in this area is on-going. In 1998 it held a Conference on Electronic Commerce, which issued a Declaration reaffirming the objectives set out in the 1980 Guidelines. In December 1999 the OECD released its *Consumer Protection Guidelines for E-Commerce*,[1060] which also recommended compliance with the 1980 OECD privacy principles.

The singular aim of the OECD *Guidelines* is to encourage free circulation of information between member countries and avoid the creation of unjustified obstacles to the development of economic and social relations between those countries. They are based on the recognition that automatic processing and trans-border flows of personal data create new forms of relationships among countries; they therefore require the development of compatible rules and practices. They also recognize that trans-border flow of personal data contributes to economic and social development, and that domestic legislation concerning privacy protection and trans-border flows of personal data may hinder such trans-border flows.[1061]

[1059] OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

[1060] OECD *Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999).

[1061] Ibid.

6.5.2 The Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data

The Convention[1062] seeks to:

> [s]ecure in the territory of each party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right of privacy, with regard to automatic processing of personal data relating to him.[1063]

This Convention is based on the recognition of the need to reconcile the fundamental values of respect for private life with free flow of information between peoples. The Convention seeks to enforce common principles of fair information practices among its members. Unlike the OECD *Guidelines* which are voluntary, the CoE Convention is binding on the signatory members.[1064] The impact of the Convention can be seen in the fact that at least forty member states have ratified the Convention to date and most of them have also enacted data protection laws modelled on the Convention. Similarly, the Convention has influenced the development of other regional data protection regimes such as the EU *Directive* and the Asia Pacific Economic Cooperation (APEC) Privacy Framework.[1065] It was the first international treaty to establish the parameters within which a person enjoyed a right to protection of his personal data.[1066] The Convention was the principal motivating force for data protection in Europe and internationally throughout the 1980s and early 90s. A subsequent protocol modified the Convention to align its provisions on TBDF and supervisory authorities with those of the European Union Directive.[1067]

[1062] Convention *for the Protection of Individuals with regard to Automatic Processing of Personal Data* (*CETS No 108*). See also Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) regarding supervisory authorities and trans-border data flows.

[1063] Art 1.

[1064] Art 4. See also the *Explanatory Report on the Convention.*

[1065] The APEC Privacy Framework was approved November 20, 2004 by APEC leaders. See the APEC Privacy Framework website [online].

[1066] Lee Bygrave refers to the Convention as the "sole international treaty dealing specifically with data protection". See Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* 32.

[1067] OECD *Report on the Cross-border Enforcement of Privacy Laws* 22.

6.5.3 Resolution 45/95 by the General Assembly of the United Nations

While the OECD and CoE guidelines were primarily Europe-focused, Resolution 45/95 adopted the United Nations *Guidelines Concerning Computerized Personal Data Files* [1068] with a worldwide target of member states of the UN. The UN guidelines were adopted by the General Assembly on December 14th 1990. In adopting the *Guidelines*, the UN General Assembly requested "governmental, intergovernmental and non-governmental organisations to respect those guidelines in carrying out the activities within their field of competence".[1069] However, the *Guidelines* are non-binding but merely provide a guide to member states of the UN on how to deal with computerised personal data files.

Resolution 45/95 of the UN under which the *Guidelines* were adopted, requested governmental, intergovernmental and non-governmental organizations to respect the UN guidelines in carrying out activities within their field of competence. The *Guidelines* lay down a number of principles concerning minimum guarantees to be provided for in national legislation or in the internal laws of international organizations and they conform to the standards set by various international instruments such as the OECD Guidelines of 1980, and the EU *Directive 95/46/EC* of 1995. Some of the principles established in the Guidelines for the handling of personal data are: the purpose-specification requirement, the principle of accuracy, consent requirements, and the requirement of availability of data to individuals.[1070]

[1068] United Nations *Resolution 45/95*.

[1069] United Nations *Guidelines for the Regulation of Computerized Personnel Data Files.*

[1070] The Principles are:

i. The purpose-specification principle states that there must be a legitimate purpose for data collection, and the use of the data collected must be compatible with the specified purpose.
ii. Data controllers have the responsibility of ensuring that data is kept up-to-date and accurate. The individual has a right to object if the information is inaccurate.
iii. Consent of the individual should be obtained before data is collected, whenever possible.
iv. Every individual should have the right to ascertain whether personal data is stored, who has access to this information, and for what purposes it is used.
v. 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.
vi. Data that is 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.
vii. Appropriate measures should be taken to protect the files against both natural dangers, such as

Like the EU *Directive 95/46/EC*, the UN *Guidelines* provide for the establishment of a competent, impartial and independent supervisory authority to oversee the protection of personal data.[1071]

6.5.4 UN General Assembly Draft Resolution: "The Right to Privacy in the Digital Age"

In November 2013, the United Nations Social, Humanitarian and Cultural Affairs Committee (The Third Committee), unanimously approved the draft Resolution "The Right to Privacy in the Digital Age" (the Resolution) which, among other things, aims to protect online and offline privacy against unlawful or arbitrary surveillance. In a statement by the Committee, "… the Resolution calls on Member States to review their procedures, practices and legislation on the surveillance of communications, their interception and collection of personal data."[1072] The Resolution also calls on Member States to "establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency […] and accountability for State surveillance".[1073] The Committee noted however, that "Some [delegates] expressed regret over the lack of a specific reference to such mechanisms in the draft".[1074] The General Assembly is expected to vote on the Resolution in December and if adopted, it will be, as noted by the Electronic Frontier Foundation, the first Resolution by the General Assembly on the right to privacy since 1988.

---

accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

1071 Guideline no 8.

1072 See Data Guidance *UN Resolution to Establish International Human Right to Privacy Online* [online].

1073 Ibid.

1074 Ibid.

6.5.5 The Charter of Fundamental Rights of the European Union

The *Charter of Fundamental Rights*[1075] of the European Union was signed and proclaimed at the European Council meeting in Nice on 7 December 2000. The Charter aims to strengthen the protection of fundamental rights in the European Union in order to enable the Union contribute to the preservation and development of the universal values of human dignity, freedom, equality and solidarity within its fields of competence.[1076] It proclaims the fundamental right to data protection as an autonomous fundamental right and declares that respect for data protection laws must be subject to control by an independent authority.[1077] It provides that:

> … [d]ata must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

The Charter also envisages the setting up of an independent authority to monitor compliance with the provisions of the Charter.[1078]

6.5.6 ECOWAS *Supplementary Act on the Protection of Personal Data within ECOWAS Region* (2010)

In 2010, the Heads of State and government of the member states of the Economic Community of West African States (ECOWAS) adopted the *Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS*.[1079] The Act was adopted in consideration of the advances in ICTs and the Internet and in recognition

---

1075 The EU *Charter of Fundamental Rights*.

1076 See the Preamble to the EU *Directive*, recitals 2, 3 and 4.

1077 Art 8.

1078 Ibid.

1079 ECOWAS *Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS,*

of the high potential to use the Internet and ICTs for profiling and tracing of individuals and also as valuable tools for collecting and processing personal data which may be prejudicial to the private and professional life of users.

The Heads of State and government of the regional organisation also noted the legal vacuum in the national laws of member states to address the issues arising from the use of the Internet as an instrument of communication, particularly in relation to personal data protection. The *Supplementary Act* was adopted to fill the vacuum by providing a harmonized legal framework for the protection of personal data collected and processed via ICTs and the Internet in West Africa. The Act requires member states to enact a legal framework of protection for data privacy relating to collection, processing, transmission, storage and use of personal data without prejudice to the general interest of each state.[1080] The ECOWAS *Supplementary Act* is patterned after the *EU Directive 95/46/EC* and like the Directive, it provides for the establishment of Data Protection Authorities in each member state.[1081]

The obligation of member states such as Nigeria, to comply with ECOWAS decisions is set out in article 9(4) of the ECOWAS Treaty[1082] which provides that:

> Decisions of the Authority shall be binding on the Member States and institutions of the Community, without prejudice to the provisions of paragraph (3) of Article 15 of this Treaty.

Similarly, article 5(2) of the Treaty provides that:

> Each Member State shall, in accordance with its constitutional procedures, take all necessary measures to ensure the enactment and dissemination of such legislative and statutory texts as may be necessary for the implementation of the provisions of this Treaty.

The above provisions of the Treaty do not appear to give member states of the ECOWAS the same kind of discretionary leeway members of the EU have in transposing the Directives of the EU into their domestic legal regime. Art. 249 sec. 3

[1080] Art 2 of the Act.

[1081] Id Art. 14.

[1082] Treaty of ECOWAS, 1975.

of the EC Treaty provides that: "A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."[1083] Thus, while EU members enjoy the discretion to consider the most appropriate means of implementing Directives into domestic law provided that the objectives of the Directives are attained and provided that the Directive is implemented into domestic law within the required timescale, ECOWAS members do not enjoy such discretion but must "ensure the enactment and dissemination of such legislative and statutory texts as may be necessary for the implementation of the provisions of this Treaty."[1084]

Because the ECOWAS Treaty and the *Supplementary Act* are patterned after the EU Treaty and EU *Directive 95/46/EC* respectively, there is provision in the ECOWAS Treaty[1085] for sanctions against members of the regional body for failure to fulfil their obligations to the organisation. No sanctions or steps towards sanctions have so far been taken against Nigeria or any other member state of the organisation for failure to adopt or enact a data protection law.

6.6 The EU Directives and TBDF

6.6.1 Uneven protection of information privacy across borders

According to Shaffer, one positive effect of globalization is that it can influence the "ratcheting up of national standards". When lax regulation in country A adversely affects the residents of country B, such laxity can prompt the citizens in country B to pressure their government to apply the state's market power to challenge foreign activities prejudicial to their interests. In the context of data protection, the collective fears by the citizens of the EU about inadequate levels of privacy protection in other countries effectively pressured their representatives in the European Commission to produce the *Data Privacy Directive*.[1086] The growing awareness of both the power of

[1083] See EU *Treaty Establishing the European Community* (2002).

[1084] Art. 5(2) Treaty of ECOWAS 1975.

[1085] Art. 77(1).

[1086] Shaffer 2000 (25) *Yale J Int'l L* 7.

information as a resource, and of the increasing volumes of personal information (or data) that was flowing between countries, gave impetus to these concerns.[1087]

The European debate sought to place some parameters on the widespread flow and use of the personal data of European citizens. These concerns culminated in the 1995 *European Union Data Protection* Directive[1088] which required members of the European Union to implement their own national privacy laws to reflect the data export restrictions in the *Directive*.

By issuing the *Directive*, the European Union placed the regulation of trans-border data flows and information privacy protection on the global agenda. The *Directive* has extraterritorial application because it prohibits the transfer of personal data of EU citizens and residents to third countries that do not have an adequate level of information privacy protection.[1089] In adopting the *Directive*, the European Union declared, in effect, that it would deny certain trade opportunities to those countries that did not meet its standards of privacy protection. Arguably, this was a move that was intended to force the rest of the world into accepting a common global privacy policy. A number of nations have since responded by enacting data protection laws.[1090] These laws *inter alia* regulate trans-border flows of personal information; their aim is to provide an added measure of protection for information privacy in those countries where data protection laws have been enacted.

The insatiable appetite of the global economy for free flow of information, coupled with the uneven protection of information privacy worldwide, resulted in the *Directive* which demands that non-EU countries work towards a global resolution of

---

1087 Ibid.

1088 *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. Official Journal L 281, 23/11/1995 P. 0031 – 0050.*

1089 The processes by which a determination is made as to the adequacy of protection in a third country will be examined in the next chapter.

1090 According to Greenleaf, as of mid-2011 there were seventy six countries that had enacted data protection laws that cover most of their private sectors and include privacy principles meeting or exceeding the minimum standards of international data protection and privacy agreements. See further Greenleaf 2011 No 112 *PL&BIR* 1 [online]. In November 2013, South Africa adopted its own data protection law, the Protection of Personal Information Act 4 of 2013.

the legal and political differences inherent in information privacy protection. The effects of trade and financial globalisations are such that few countries are able to insulate themselves from the daily operations of the global markets. As governments and businesses collect, process, store and use huge amounts of personal information, the threats to information privacy continue to increase.[1091] Because of these risks, the regulation of trans-border data flows at national and international levels is now a policy option that governments across the world can no longer ignore.

Although many countries have enacted laws that limit the processing and disclosure of personal information, privacy breaches and identity thefts continue to increase.[1092] On the one hand, this may be due to weak or ineffective enforcement of the data protection laws in countries where they are available. On the other hand, inconsistencies in the levels of protection or outright absence of legal protections in some countries constitute major obstacles to the protection of trans-border flows of personal information.

Reidenberg[1093] argues that specific privacy rules have a governance function; they are either liberal, market-based privacy rules or socially protective, rights-based rules. The inconsistencies or conflicts in levels of protection may be due to differences in constitutional standards and cultural attitudes toward privacy in different countries.[1094] If left unresolved, these differences will constitute impediments to the free flow of information in the global economy. Because of these structurally divergent approaches to information privacy protection, international harmonization of the regulation of trans-border data flows becomes imperative.

6.6.2 The extraterritorial application of EU Directives on data protection

---

[1091] These threats are compounded by the fact of trans-border flow of information between states. The risks to individuals include exposure to identity theft, damage to reputation and loss of personal information privacy if such information is used contrary to data protection laws or the individual's own privacy preferences.

[1092] See Privacy Rights Clearinghouse *Identity Theft and Data Breaches* [online].

[1093] Reidenberg 2000 (52) No 5 *Stan L Rev* 1320.

[1094] Milberg, Smith and Burke 2000 (11) No 1 *Organization Science* 35-57. See also Walczuch, Singh and Palmer 1995 (8) No 2 *Inform Tech & People* 37.

In 1995, the European Union passed *Directive 95/46/EC*,[1095] under which member states were required to enact implementing legislation. The *Directive*, and the enactments made pursuant thereto, represents the most ambitious and far-reaching data privacy initiative to date.[1096] Like all EU *Directives*, it is not in itself a law; rather, it directs each of the members of the European Union to enact its own implementing legislation, which need not be identical across member states in many of its specifics. According to its preamble, the *Directive* was born partly out of a desire to preserve rather than to inhibit data flows.[1097]

The European Union was concerned that data protection laws might be evaded through cross-border operations and that data flows within Europe could be hindered if the rules were not standardized across member states.[1098] By requiring similar data privacy protection throughout the Union, the *Directive* removed the threat to the free movement of personal data between member states, on grounds relating to protection of the right to privacy.[1099] The threat to the free movement of personal data now stands between the European Union and third countries like Nigeria with questionable levels of data protection. Article 25 of the *Directive* requires member states of the EU to prohibit the transfer of personal data to a third country that does not ensure an "*adequate*" level of protection.

This *Directive* is also based on the need, within the context of the European Union, to avoid any obstacle to the free flow of personal data between the member states. The protection of the rights and liberties of individuals and, in particular, their right to privacy, was seen as a possible barrier, because of the differences between the levels of protection of those rights in member countries. Such differences might constitute a hindrance to the exercise of a series of economic activities throughout the Union and thereby interfere with competition. Under the *Directive*, the transfer

---

1095 The EU *Directive 95/46/EC.* See also *Regulation (EC) 45/2001* and *Directive 2002/58/EC* (Directive on Privacy and Electronic Communications).

1096 Salbu *The European Union Data Privacy Directive and International Relations* 1 [online].

1097 See n 1088 at Preamble par 1.

1098 See n 1086 at11.

1099 See n 1088 at Preamble par 9.

of personal data within the EU and EEA may not be restricted[1100] on the basis of the level of data protection available in a member state, whereas it prohibits the transfer of personal data to non-member states of the EU.

6.6.2.1 Directive 95/46/EC

The *Directive* protects "personal data," which is defined as "any information relating to an identified or identifiable natural person."[1101] An identified or identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[1102] The *Directive's* restrictions apply to data collectors who engage in personal data processing which is defined as operations or sets of operations that are performed on personal data, automatically or otherwise.[1103] It includes, but is not limited to, "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[1104]

The territorial scope of the *Directive* is prescribed by article 4; it makes the *Directive* applicable to data processing if "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State".[1105] Where therefore, an individual or company (the data controller) has an establishment[1106] located in Europe that is engaged in processing data either for

---

1100 See art 1(2).

1101 Art 2(a).

1102 Id art 2(c).

1103 Id art 2(b).

1104 Ibid.

1105 Art 4(1)(a) provides that where:

> [T]he 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 the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

1106 Although *Directive 95/46/EC* does not define the term "establishment", its Preamble explains the ambit of

himself/itself or on behalf of another person or company, for export to a third country, such processing falls within the purview of article 25(1) of the Directive.[1107]

The basis for determining the applicability of article 25(1) of the *Directive* to the processing of personal data is the physical presence of the data processor in the territory of a member state of the EU. Thus, when the processing is carried out in the context of the activities of an establishment of the controller on the territory of one member state, the data protection law of that member state applies to the processing. In that context, it is safe to say that the Directive has little or no extraterritorial reach even though it has an external effect by prohibiting the transfer of processed data to third countries.[1108]

The foregoing notwithstanding, the extraterritorial effect of the *Directive* can be seen where a data processor is located outside of Europe but takes full control of processing equipment located in Europe and uses the equipment directly for the collection of personal data without the consent of the Europe-based data subject. Using the example of Firstbank Plc noted above, such collection by non-EU based data processors is where Fistbank's website puts a cookie on the personal computer of individuals in the EU in order to identify the PC to the web site whose server is located in the UK, with a view to linking up that information with others. Such collection and processing of data may become subject to the restrictions of article 25.[1109]

---

the term by stating that establishment "implies the effective and real exercise of activity through stable arrangements". However, the legal form of such an establishment is not the determining factor in this respect". See the *Preamble*, recital 19.

[1107] Article 25(1) provides that:

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

[1108] See Poullet 2007 (2) *JICLT* (2007) 145-146. See also n 977 at 12. Coughlan *et al,* make the point that some legislative or judicial action may have an impact or influence outside the legislating country's geographical borders but nonetheless, they ought not to be considered as truly "extraterritorial" because the extraterritorial impact is coincidental. Such is the case with *Directive 95/46/EC* in so far as it concerns the processing of personal data by a data controller located within the EU.

[1109] Art 4 provides that where:

> (1)(c) the controller is not established on 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

According to the Working Party,[1110] the *Directive* applies when the controller is not established on EU territory, but decides to process personal data for specific purposes and makes use of equipment, automated or otherwise, situated on the territory of a member state.[1111] However, the Working Party recommended a cautious approach to the application of article 4(1)(c). The objective of the article is to ensure that individuals enjoy the protection of national data protection laws and the supervision of data processing by national data protection authorities "in those cases where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved.[1112]

6.6.2.2 Directive 2002/58/EC (Directive on privacy and electronic communications)

In 2002, the European Parliament and the Council of the European Union passed a new Directive on privacy and electronic communications[1113] (*Directive on Privacy and Electronic Communication*), which went into effect on October 31, 2003. The Directive seeks to ensure an equivalent level of protection of privacy rights among the member states with regard to personal data processing in the electronic communication sector. It is also meant to ensure the free movement of such data and

---

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 that Member State, without prejudice to legal actions which could be initiated against the controller himself.

See Poullet n 11108 at p 146.

[1110] Article 29 of *Directive 95/46/EC* establishes a Data Protection Working Party ('Working Party'); the Working Party is an expert body made up of representatives from the data protection authorities of EU member States. One of the tasks of the Working Party is to "give the Commission an opinion on the level of protection in the Community and in third countries" (art. 30(1)(b)). It is also required to "draw up an annual report […] regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission" (art. 30(6)).

[1111] Article 29 Working Party *Working Document on the Applicable Law in case of Personal Data Processing by non-EU Web Sites* 7.

[1112] Ibid at 9.

[1113] *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* (*Directive on privacy and electronic communications*).

of electronic communication equipment and services in the EU.[1114]

Directive 2002/58/EC translates the principles set out in *Directive 95/46/EC* into specific rules for the electronic communications sector by laying down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services.[1115] Unlike *Directive 95/46/EC*, the *Directive 2002/58/EC* fully takes into consideration recent advances in the deployment of Internet services and the global nature of its infrastructure.[1116] It recognizes the risks to information privacy inherent in TBDF through the infrastructure of the Internet. It also recognizes the fact that European users of the global telecommunications infrastructures such as the Internet are exposed to risks beyond the risks generated by the operations of data controllers established in EU countries.

Because the traffic and location data pertaining to Europeans may be collected, processed and transmitted unlawfully by telecommunications services providers established outside of the EU, *Directive 2002/58/EC* targets all electronic

---

[1114] Id art 1(1).

[1115] See Articles 5, 6 and 9 of the *Directive*:

> Art 5(1): Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1).
>
> Art 6(1): Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).
>
> Art 9(1): Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

[1116] Preamble, recital 5 and 6 *Directive 2002/58/EC.*

communications services without any distinction as to the nationality or the place of establishment of the providers.[1117] To that extent, the Directive clearly evinces an extraterritorial scope.[1118]

As noted in its Preamble, *Directive 2002/58/EC* acknowledges that:

> New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the Information society is characterized by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk."[1119] (Underlining supplied)

The observation that access to digital mobile networks has become available and affordable for a large public is not only true of the member states of the EU, but it is true also of many countries outside the EU. The phenomenal increase in the last decade, of access to digital telephony in Nigeria is a good example. With a mobile phone penetration in excess of 100 million subscribers, Nigeria has made a very significant effort to join the Information Society.[1120] However, it still lags far behind in terms of providing a regulatory framework for protecting the data privacy of its growing subscriber base of fixed and wireless telecommunication users. For Nigeria, the *lacuna* in regulatory protection of informational privacy is all the more worrisome given the fact that a culture of human rights protection has not yet been entrenched in the polity. Moreover, 99% of Nigeria's installed telephone capacity is

---

[1117] Art 3 provides:
(1) This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

[1118] Poullet "Directive 2002/58/EC " 164.

[1119] Preamble, recital 5.

[1120] At the end of August 2012, the total number of active fixed wired/wireless lines in Nigeria stood at 105, 239,815 lines. See NCC website [online].

of the GSM wireless technology type, which, though digital and encrypted, are nevertheless susceptible to interception.[1121] In sharp contrast to the comprehensive regulation and protections contained in *Directive 95/46/EC* and *Directive 2002/58/EC,* the Nigerian Communications Act[1122] which regulates telecommunications services in Nigeria, is virtually silent with regard to the protection of information privacy of users of the telecommunications services. A brief comparison of the Directives and the Act makes this clear.

Article 10 of *Directive 95/46/EC* provides that member states shall require organisations that collect personally identifiable information to reveal:

- the identity of the controller[1123] and of his representative, if any,
- the purposes of the processing for which the data are intended,
- any further information such as the recipients or categories of recipients of the data, etc.[1124]

[1121] For example, Mark Odell of the *Financial Times* reported that once police or the security services know the mobile phone number of a suspect, they can ask the mobile operator to track the individual. As long as the handset is switched on the telephone can be tracked across any mobile network in real time. Odell 2nd August 2005 *Financial Times*. Similarly, the recent phone hacking scandal involving the *News of the World* newspaper in 2011 shows quite clearly that mobile telephony is as easily susceptible to interception as the old analogue phones, notwithstanding their sophistication. See Chandrasekhar, Waldrop and Trotman 23rd July 2012 *The Telegraph.*

[1122] Laws of Federation of Nigeria, 2004.

[1123] Article 2(d) defines a "controller" as "the natural or legal person, public authority, agency or any other body which alone or with others determines the purposes and means of the processing of personal data. Under the *Directive*, these disclosures are required regardless of whether the collection of data is obtained directly from the data subject or from other sources.

[1124] Subscribers are required to be well informed in the following circumstances:

i. where "So-called spyware, web bugs, hidden identifiers and other similar devices…" "…are to be used in the course of providing a service, "…the use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned." (Preamble, recital 24).
ii. where "cookies" are intended to be used "… for a legitimate purpose such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using." (Preamble, recital 25).
iii. where the data relating to subscribers contain "information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons… Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform…" (Preamble, recital 26)

The notice requirements of the EU *Directives* ensure that any user of electronic communications services who is the subject of data collection is entitled to be notified of that fact and of the party or organization that is collecting the information.

Recognising the risks to personal information privacy inherent in the use of electronic communication services, *Directive 2002/58/EC* requires service providers to take appropriate measures to safeguard the security of their services, and "inform subscribers of any special risks of a breach of the security of the network."[1125] In comparison, although the Communications Act imposes an obligation on a licensed operator to use its best endeavours to prevent its network facilities or network service from being used in or in relation to the commission of any offence under any law in operation in Nigeria,[1126] it does not require service providers to inform users of the services of any risk of breach or actual breach of security of the networks. When a subscriber is made aware of the risk to the security of his personal information, he is put in a position where he can take steps to mitigate the potential damage or loss that may arise from the breach of the network security. Information privacy is essentially about being able to control access to one's personal information.

Furthermore, Directive 2002/58/EC requires communications service providers, websites and online service providers to obtain consent from subscribers before using traffic data relating to such subscribers for the purpose of marketing electronic communications services or for the provision of value added services.[1127] By requiring that users of electronic communications services be provided with full and relevant information about the collection, processing and storage of personally identifiable

---

[1125] Preamble, recital 20. See also art 4 and 4(2).

[1126] S 146(1). A licensed operator is required to assist the NCC or other authority:

> "as far as [is] reasonably necessary in preventing the commission or attempted commission of an offence under any written law in operation in Nigeria or otherwise in enforcing the laws of Nigeria, including the protection of the public revenue and preservation of national security ." (S146(2)).

[1127] Art 6(3). The *Directive* further provides that:

> The provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

information capable of being linked to the users and the right to give or withhold their consent thereto, the Directives have given back to the users, a measure of control over their personal information which places them in a position to make well-informed choices about the uses to which their personal information can be put. This is a fundamental characteristic of the concept of information privacy.

In contrast, the Communications Act does not require telecommunications service providers in Nigeria or online service providers to notify end-users about the collection of personally identifiable information.[1128] There is also no obligation on communication service providers to notify users of breach of security of their stored personally identifiable information. Unlike the EU *Directives* that give a right of legal action against service providers failing to protect the privacy interests of their users, users in Nigeria are left without an enforceable legal remedy against service providers who are complicit in the breach of the data privacy of their subscribers.
Another worrisome defect in the Communications Act is that it does not regulate the interception of private communications in Nigeria. The Act provides that the regulator of the telecommunications industry, the Nigerian Communications Commission (NCC) may determine that a licensee or class of licensees "shall implement the capability to allow authorised interception of communications and such determination may specify the technical requirements for authorised interception capability".[1129] While the NCC has so far not made any determination for any of the telecommunications service providers to implement such a capability for authorised interception, it has failed to publish the rules and procedure that will guide it in making such a determination should the need arise in future. As the law stands today, and in the light of the many security threats facing the government and people of Nigeria, private communications may be intercepted either by the government or private entities without clearly defined rules guiding such

[1128] There are however, websites of some well-known Nigerian business entities that have taken to displaying their online privacy policies, perhaps to show that they operate according to international best practices. These privacy policies are of doubtful utility to users whose personal information is collected, processed or stored as there is no access to the database of the company that collected the information.

[1129] S 147. See also s 148 which empowers the NCC to issue an order stipulating that any communication or class of communications to or from any licensee, person or the general public, relating to any specified subject, either shall not be transmitted or shall be intercepted or detained on grounds of national security or in the public interest.

interception.

In contrast, article 5(1) of the *Directive 2002/58/EC* requires member states to "ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation."[1130] EU countries have, since the enactment of the *Directive*, transposed the provisions of the *Directive* into their national laws for the protection of electronic communications. It would be greatly beneficial to Nigerian users of electronic communications services, if a data protection law is passed to protect the information privacy of users of the communications services using *Directives 95/46/EC* and *2002/58/EC* as models. The Economic Community of West African States (ECOWAS) adopted a model data protection law in 2010, contained in the *Supplementary Act on Personal Data Protection within ECOWAS*. The Act sets out the required content for any data protection law to be enacted in any member state and it is strongly influenced by the EU Directives on data protection.[1131] Each member state is expected to enact data protection laws that would establish a data protection authority in each country.

6.7 Reform of EU data protection law

The European Commission has indicated its intention to reform EU laws on data protection. In January 2012, the Commission published its proposal for the legislative reform. The draft proposal seeks to address the challenges posed by advances in Internet technology, thereby safeguarding personal data privacy even in the face of anticipated and not so anticipated future advances in the digital environment.[1132]

[1130] In addition, member states "shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)" (Article 5(1).

[1131] See par 6.5.6 above. See also Banisar 2010 (16) *EAJP&HR* 136. See also Greenleaf 2012 (2) *IDPL* 68-92.

[1132] For example, when *Directive 95/46/EC* was enacted in 1995, Internet-based business models such as Hotmail, Yahoo, Google and Facebook were not in existence. The activities of companies such as Google and Facebook have seriously challenged the capacity of the data protection laws based on the *Directive 95/46/EC*. Also, the number of Internet users has increased dramatically while the number of Internet-enabled devices such as smartphones and tablets has also increased exponentially. According to Hammadou Toure, the Secretary-General of the ITU, "At the beginning of the year 2000 there were only

There are two proposed legislative reform packages: (a) a proposal for a regulation on the Processing of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)[1133] and (b) a proposal for a Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for Criminal Offenses.[1134] It is proposed that a Regulation, not a Directive will be enacted to replace the current Directive. The effect will be a direct application of the new law in the member states. According to the Explanatory Memorandum issued by the EU Commission, the basis for proposing direct regulation are the fragmented implementation of *Directive 95/46/EC* in different European jurisdictions and the consequent overlapping regulations that confront businesses in the EU region with the attendant cost consequences.[1135]

7. SIGNIFICANCE OF THE GLOBAL DATA PROTECTION REGIME FOR NIGERIA

Nigeria does not have a data protection law. It is not a major global economic power. Although its trade with the EU is significant,[1136] it is comparatively below that of many other countries. Nevertheless, the trade relationship between the EU and Nigeria will necessitate the transfer of personal information between the two trading partners, particularly in the services sector. The adequacy of Nigeria's level of data protection will then become an issue and a potential trade barrier. Nigeria has so far not engaged, in a significant manner, in the debates touching on the policy issues that have arisen as a result of trans-border data flows, either globally or at the national level. Nevertheless, it is steadily building up the basic telecommunications

---

500 million mobile subscriptions globally and 250 million Internet users," he said. "By the beginning of this year 2011 those numbers have mushroomed to over five billion mobile users and two billion subscribers to the Internet." See *Independent* newspaper "Number of Internet users worldwide reaches two billion: UN" 26th January 2011 [online].

1133 The European Commission *Draft General Data Protection Regulation* (2012).

1134 European Commission *Draft Regulation on Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Parties and the Free Movement of Such Data* (2012).

1135 See European Commission *Explanatory Memorandum*.

1136 See European Union *Trade with the World and EU Trade with Nigeria* [online].

infrastructures that enable these flows of information in and out of Nigeria. While some of the reasons for non-engagement have been examined in chapter 4, it remains to be said that the sooner Nigeria addresses the policy issues implicated in trans-border data flows and puts appropriate policy instruments in place, the better prepared it will be to fully integrate into the global network economy.

Although Nigeria is not an EU member country, the EU *Directive* may have an impact on it in two ways:

- Article 25 of the EU *Directive* prohibits EU nations from transferring personal data to third countries which do not guarantee adequate protection of such data. Given the fact of the inadequate level of data protection in Nigeria at present,[1137] the Article clearly prohibits a direct transfer of personal data from any EU member country to Nigeria, unless the relevant exceptions apply.[1138]

- It is arguable that the EU Directive will also have the effect, in a third country, of restriction against onward transfers of data to fourth countries which do not guarantee adequate data protection. Other countries that want to ensure the free flow of personal data from EU countries would enact data protection laws having in them restrictions prohibiting the transfer of data to countries without adequate data protection regimes. For example, if Ghana were to enact a data protection law with a clause similar to Article 25 of the EU Directive, this would restrict the flow of data to Nigeria, not only of Ghanaian citizens, but also of EU citizens' data transferred from Europe to Ghana.

Historically, trans-border data flows have always elicited one form of regulation or restriction or another. States have not liked the idea of allowing free and unregulated flow of information across their borders.[1139] Consequently, diverse national barriers have been erected and continue to be erected against free trans-border data flows. These barriers are usually justified on grounds such as privacy, taxation, national

---

[1137] See chapter 4.

[1138] Note that under article 25(2) and 26(2) of *Directive 95/46/EC*, any regulatory regime, including contractual provisions, self-regulatory systems or even technological means might be taken into consideration in determining whether adequate protection is available in a third country.

[1139] Lowry 1984 (6) *Hous J Int'l L* 164.

security, cultural preservation and national sovereignty. Some have argued that privacy plays a minor part in trans-border data flows, particularly with regard to multinational corporations and their operations. They see the agitation for regulation on grounds of privacy as "just a convenient club with which to beat to death the freedom to exchange information."[1140]

According to Novotny[1141] national security justifications for restrictions on trans-border data flows are often exaggerated. "National security" should not be interpreted so widely as to stop the free flow of information.[1142] There is however consensus on the need for all information collection to be subjected to the Fair Information Principles, particularly the disclosure principle[1143], which lies at the core of information privacy protection. The FIPs seek to establish a balance between the need for free flow of information and the individual's desire to withhold personal information.

The international instruments on data protection enumerated above are all based on and promote the Fair Information Principles that define the essence of information privacy. The instruments are mostly non-binding and have little direct legal effect in the different jurisdictions of the member states that accede to these soft law instruments. Nevertheless, all of the instruments taken together have contributed immensely to the development of data protection law in the last 30 years.[1144]

1140 Id at 166.

1141 Novotny 1980 (16) *Stan J Int'l L* 166.

1142 Id at 167.

1143 Individual Participation Principle: 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 within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs(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. See Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

1144 Greenleaf 2012 (2) *IDPL* 68-92.

Two questions that arise from the foregoing are: what are the implications of the global regulation of trans-border data flows for Nigeria and how should the country respond to the current trends in global regulation particularly as represented by the EU *Directives*? These are some of the issues that will be addressed in the next chapter.

CHAPTER 7

INTEGRATING NIGERIA INTO THE GLOBAL NETWORK ECONOMY THROUGH LAW REFORM

1. INTRODUCTION: IMPORTANCE OF INTEGRATION INTO THE GLOBAL NETWORK ECONOMY FOR ECONOMIC DEVELOPMENT

At the beginning of this thesis,[1145] it was argued that accessing the global network economy demands a network presence. That reality is re-echoed here - Nigeria must plug into the global network economy or risk being shut out. Accessing and integrating into the global network is crucial for Nigeria's development. As a developing country, and at the nascent stage of technological development, Nigeria cannot afford to ignore the global market economy and the benefits that its empowering technologies such as the Internet and ICTs offer.

The massive integration of global markets for capital, goods and services, knowledge and labour across national borders, is one of the more significant transformations resulting from globalisation in the last three decades. International trade is driving the diffusion of goods, services and technologies and consequently, global integration. Being an active member of the global network economy is essential to Nigeria's economic growth. That is why Nigeria aspires to be a major economic hub of the African continent. For this aspiration to be realised however, the country must interface with the global economic system and integrate itself into the global networked economy.

It is common to find in the literature on international trade and economic growth almost invariably, arguments in support of the benefits of free trade for promoting

[1145] See chp 1 par 1.1 above.

economic growth while at the same time integrating countries into the world economy.[1146] Todaro[1147] for example, argues, with particular reference to developing countries, that trade allows access to global markets which provide these countries with development opportunities that would not be available otherwise. Trade is therefore considered to be an important stimulator of economic growth and open trade is believed to promote economic welfare.[1148] Arguments supporting the positive effect of trade openness on economic growth date back to Adam Smith's analysis of market specialisation.[1149] Proponents of trade openness argue that it promotes the efficient allocation of resources through comparative advantage, allows the dissemination of knowledge and technological progress, and encourages competition in domestic and international markets. Andersen and Babula, in support of trade openness, have noted that significant growth rates are often associated with countries that embrace globalisation and open themselves to the international exchange of goods and services as well as ideas and technologies.[1150]

Against this background, two major developments on the world scene in recent times have underlined not only the importance of international trade to national development, but have also established the nexus between trade and technology. First, the importance of trade in promoting economic growth resulted in the steps taken towards the gradual removal of trade barriers under the *General Agreement on Tariffs and Trade* (GATT)[1151] and the *General Agreement on Trade in Services*

1146 Soubbotina and Sheram *Beyond Economic growth: Meeting the Challenges of Global Development* 67-70. See also Grossman and Helpman "Technology and Trade" [online]; Chang, Kaltani and Loayza 2009 (90) *J Dev Econ* 34-35; Todaro and Smith *Economic Development* (8th ed) (2003).

1147 Todaro and Smith *Economic Development* chp 12.

1148 Ibid.

1149 Chang, Kaltani and Loayza 2009 (90) *J Dev Econ* 34-35.

1150 Andersen and Babula "Openness and Long-Run Economic Growth" 2-3 [online]. Although they concede that international trade facilitates technological development, they nevertheless question how strong the correlation between openness and economic growth is and whether international trade liberalization is sufficient to ensure sustained improvements in living conditions in developing countries.

1151 The GATT was an inter-governmental treaty between nation states and customs territories, and became the permanent institutional basis for the multilateral world-trading regime that has prevailed to this day. At the initial signing of the agreement, there were 23 signatories, which number had grown to almost 130 by the end of 1994. As a result of these negotiations, average world tariffs on manufactured goods were reduced

(GATS).[1152] Second, and a more recent development, has been the birth and fast growth of trade in the electronic medium (e-commerce), as a result of the recent advances in ICTs. The growth of trade in services in the global economy, coupled with the rising use of ICTs, provides developing countries new avenues for participation in global trade. Participation is however dictated by adherence to evolving regulatory regimes[1153] that are gaining greater importance and power as the process of globalisation deepens.[1154] Of particular concern to this chapter is the emergence of information privacy protection as a regulatory regime exerting influence on contemporary international trade relations and the impact that the regime and other regulatory regimes have had and continue to have on international trade since the advent of the EU's Directive 95/46/ EC. These regulatory regimes require all the participants in the global market network to adhere to the standards set.

---

from 40% to about 6.3%. Attention was then directed to non-tariff trade barriers for the first time during the Tokyo Round that ended in 1979. Such barriers included government procurement policies, subsidy policies, customs valuation policies, and technical standards. See generally, the WTO website for more information on GATT [online].

[1152] The *General Agreement on Trade in Services* (GATS) was one of the remarkable achievements of the Uruguay Round of negotiations under the GATT. The conclusion of the GATS reflected a firm belief in the role of free trade in promoting economic welfare. The Agreement was drawn with the basic purpose of establishing a multilateral framework of principles and rules for trade in services with a view to the expansion of such trade under conditions of transparency and progressive liberalization. The GATS is structured so that each WTO member makes its own individual commitments on opening up its services sector to competition from foreign suppliers. It permits member countries to undertake progressive opening of service sectors and integration into the multilateral trading system at their pace. The nature and extent of the GATS commitments are matters of choice for WTO member governments. They are policy issues based on members' assessments of their national development needs, strategy and priorities. Under the GATS, Nigeria made commitments in respect of financial services, particularly in most of the core sectors of banking business. See Oyejide and Bankole *Liberalisation of the Services Sector in Nigeria* 22-26 [online].

[1153] The global trade environment that the Uruguay Round (which gave birth to the WTO) engendered gave weight to some of the rules that impinge directly on domestic policies and practices, such as the rules relating to foreign direct investment (FDI) and subsidies. This new environment necessitated the revisions of domestic laws and regulations to accommodate the liberalization of the service industries in order to achieve deeper integration of markets. According to Brown and Stern, this marked the beginning of a new development in trade relations in which actual or proposed rules of the WTO could penetrate more deeply into the management of national economic and social affairs. See Brown and Stern *Global Market Integration and National Sovereignty* 11 [online].

[1154] As noted in the previous chapter, contemporary globalisation of trade has transformed state autonomy and induced shifts in state policy. The ability of nations to formulate and enforce national policies in support of and for the protection of domestic industries is increasingly subject to international scrutiny and regulation. See Held, Mcgrew, Goldblatt and Perraton *Global Transformations: Politics, Economics and Culture* 188.

.

2. REGULATORY STANDARDS AS BARRIER TO INTEGRATION

2.1 The link between trade, international standards and market access

As noted by Kobrin, while the information revolution facilitates integration by removing, or limiting, the barriers posed by physical distance and geography, it places greater emphasis on competition and on an appropriate policy/regulatory framework. Standards, particularly for technology, have become a significant factor in international trade.[1155] National standards have been used legitimately by many countries to advance their economic development and national competitiveness objectives. However, national standards can also be used to protect domestic industries from global competition and thereby constrain market access, particularly for developing countries with weak standards.

The WTO's *Agreement on Technical Barriers to Trade* ("TBT Agreement")[1156] recognises the important contribution that international standards can make by improving efficiency of production and facilitating international trade. The treaty also cautions that standards should not be used to create unnecessary barriers.[1157] The presence of multiple standards, or of a required national standard differing from existing international standards, can significantly increase costs for foreign firms, or severely limit their market access.[1158] According to Colin Scott,[1159] standards express at least some aspect of the behaviour which participants in the regime are intended to adhere to. A broader conception of standards defines them as instruments which encourage the "pursuit or achievement of a value, a goal or an outcome, without specifying the action(s) required"[1160] to achieve this, in contrast with a legal rule,

---

1155 Gibson "Globalization and the Technology Standards Game" 2 [online]. According to an OECD study in 1999, up to 80% of global trade (equivalent to about $4 trillion annually) is affected by standards or associated technical regulations. See OECD *Regulatory Reform and International Standardisation* 4.

1156 WTO *Agreement on Technical Barriers to Trade* (1994), Annex 1A to the Marrakesh Agreement Establishing the World Trade Organization.

1157 Ibid. See the preambles to the treaty.

1158 See n 1155 at 43-47.

1159 Scott *Standard-Setting in Regulatory Regimes* 1 [online].

1160 Braithwaite and Braithwaite 1995 (4) *Soc Leg Stud* 307.

which is prescriptive as to what its subject must or must not do.

The multiplicity of international and national standards impacts the efforts by developing countries to gain access to global markets and exerts pressure on their governments to improve their regulatory frameworks to meet international standards. The WTO, in its report on world trade in 2005, noted that:

> Change in the standardization field is putting pressure on governments in developing countries to reform and develop their standardization infrastructures. … National standardizing bodies are in many cases governmental bodies weakly linked to markets and largely inward-oriented. African standardization bodies, for example, had produced an average of only 1,281 standards in total by the end of 2002, while the corresponding figure for Western European bodies was 15,407.[1161]

According to the United Nations Industrial Development Organisation (UNIDO), the complexity and extent of the problems associated with standards in global trade is demonstrated by the fact that the worldwide stock of standards and technical regulations is above 100,000 and still growing.[1162] The organisation, while acknowledging that standards and technical regulations provide many important advantages to producers and consumers, both in domestic and export markets, also noted that in many cases, they have become stumbling blocks hindering market access for developing countries.

International standards and regulatory frameworks have thus become technical and non-technical barriers that developing countries like Nigeria must overcome in order to integrate fully into the global network economy in the 21st century.[1163] What developing countries need, according to the UNIDO, are adequate physical and institutional infrastructures and the skills to enable them to meet international standards. Such capacities are however, rarely available in developing countries. Extant global standards and regulatory regimes require the participants in the global

---

[1161] World Trade Organisation *World Trade Report: Exploring the links between Trade, Standards and the WTO* (2005) xxxii.

[1162] United Nations Industrial Development Organisation (UNIDO) *Enabling Developing Countries to Participate in International Trade: Strengthening the Supply Capacity* 2.

[1163] Oyejide, Ogunkola and Bankole "Quantifying the Trade Impact of Sanitary and Phytosanitary Standards: What is Known and Issues of Importance for Sub-Saharan Africa" 13.

network economy to fully satisfy the regulatory standards. Developing countries in particular, are compelled to respond to these regimes by raising their standards, in relation to globally accepted norms, or where no standards exist, to establish such by reference to global benchmarks.

The global market network that Nigeria seeks to connect to is a flexible inter-connected system centred on multinational corporations, global financial markets and a highly concentrated system of technological research and development.[1164] According to Castells,[1165] the extreme flexibility of the system allows it to link up everything that is valuable according to dominant values and interests, while disconnecting everything that is not valuable, or becomes devalued.[1166] This simultaneous capacity to include and exclude people, territories and activities is based upon a capacity to network in accordance with the dominant value and interests usually set by the most powerful group or groups in the system.

The most critical distinction in the organisational logic of inter-connected networks is to be or not to be in the network.[1167] Being in the network ensures that a developing country can share in the flow of money, information, technology, goods, services and people. To be out of the network, or become switched off, ultimately diminishes a developing county's chances of development since everything that counts is organized around a worldwide web of interacting networks.[1168] It must be emphasized however, that being a part of the global network requires adherence to the dominant values and standards that regulate the parameters of interaction within the network.[1169]

[1164] Castells *nformation Technology, Globalization and Social Development* 6-7 [online].

[1165] Ibid.

[1166] Ibid at 6.

[1167] Ibid.

[1168] Ibid.

[1169] See n 1164 at 12. The values and interests that regulate the parameters of operation of the networks are dictated by the major trading partners in the network such as the US, the EU and Japan. These values and interests, operating by way of rules, place restrictions on the freedom of governments to discriminate in favour of national companies or industries through the use of domestic measures. The objective of the leading members of the WTO is to create an international framework of rules and procedures within which their own markets could be more closely integrated with each other. It is, as Brown and Stern put it, to establish a "level playing field" in which the firms of each country would ideally compete everywhere on

2.2 Data protection legislation as barrier/gateway to the global network economy

To succeed in the twenty-first century, Nigeria has to become a full partner in the global network economy. However, as argued earlier, integrating into the global network economy demands that Nigeria abides by the rules of the network. The rules are largely set by the dominant players in the network; data protection is a critical component of the regime of rules and regulations that govern the global market network. Among the wide variety of national and multinational legal regimes for protecting privacy, two dominant models have emerged, reflecting two very different approaches to the control of information. At one end, there is the sweeping data protection model adopted by the members of the European Union. It imposes significant restrictions on data collection, processing, dissemination, and storage activities, not only within Europe, but throughout the world if the data originates in a member state.

At the other end of the privacy protection spectrum is the policy of the US that extensively regulates the processing of data by government, while facilitating private, market-based initiatives to address private sector data processing. In between the two major policy approaches are hybrid combinations of state regulation and market-based self-regulatory measures.[1170]

One of the more dominant values or standards dictating the terms of interaction and integration into the global network economy in modern times is the data protection regime set up by the European Union.[1171] The EU *Directive* has elicited regulatory responses and influenced legislation in New Zealand, Canada, Australia, Hong Kong and several other countries.

---

the same terms. See Brown and Stern *Global Market Integration and National Sovereignty* 11.

[1170] Singapore for example, is generally characterized as having a self-regulatory data protection framework. The country's Model Data Protection Code is voluntary. See Chik 2006 (14) *IJLIT* 47–100.

[1171] In 1995, the European Union passed the *Data Protection Directive* that set out to create a common European framework of data protection principles that will protect the information privacy of its citizens. The *Directive* also seeks to restrict the movement of individuals' personal data to countries outside the European Union that do not have "adequate" privacy protection. See the EU *Directive 95/46/EC, Regulation (EC) 45/2001* and *Directive 2002/58/EC* (*Directive on Privacy and Electronic Communications*).

At a conference held in Montreux, Switzerland in 2005,[1172] Data Protection and Privacy Commissioners around the world adopted the *Montreux Declaration*,[1173] at the end of the conference, which recognised the increasing importance and cross-border context surrounding international data transfers and the disparity in national and regional data protection regimes. The Declaration accepts the protection of privacy as a fundamental human right[1174] and therefore recommended the preparation of a convention that will strengthen the universal character of data protection principles. In the *Declaration*, the Data Protection and Privacy Commissioners appealed "to every government in the world to promote the adoption of legal instruments of data protection and privacy according to the basic principles of data protection and also to extend it to their mutual relations."[1175]

The Data Protection and Privacy Commissioners called on the United Nations to prepare a convention on data protection that will recognise the universal nature of privacy rights and data protection. The proposed convention will seek to overcome the inconsistencies and barriers to cross-border information transfers created by divergent data protection regimes. Participants at the conference also considered the need for international mechanisms to protect personal data and the importance of self-regulation in implementing data protection principles.[1176] One of the major characteristics of data protection legislations, particularly the EU *Directive* on data

---

1172 The 27th International Conference of Data Protection and Privacy Commissioners (Montreux, Switzerland, 14-16 September 2005). See conference website [online]. The Conference was attended by Privacy and Data Protection Commissioners from more than 40 countries and over 300 participants from business, public administration, the IT industry, government and non-government organisations attended the conference.

1173 Montreux Declaration*: The Protection of Data and Privacy in a Globalised World: A Universal Right Respecting Diversities.*

1174 Movius and Krup 2009 (3) *IJoC* 172. To many Europeans, privacy is an inalienable human right which should be beyond the marketplace and should not be traded. Most Americans however, see the privacy of their personal information as a commodity which can be bought and sold.

1175 See n 1173. Similar appeals were made at the data protection commissioners' conference held in Strasbourg in 2008. See *Resolution on the Urgent Need for Protecting Privacy in a Borderless World, and for reaching a Joint Proposal for setting International Standards on Privacy and Data Protection* (2008).

1176 Another significant call by the Data Protection and Privacy Commissioners is for the Council of Europe to invite non-member states to accede to the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. The Council of Europe has opened accession to the Convention to non-member States. See Council of Europe Committee of Ministers, 1031st meeting (2 July 2008), *Decision Item 10.2*. However, by the decision of the Council, accession to the Convention by non-member States of the Council of Europe is only open to those with data protection legislation that is in accordance with the Convention. This requirement greatly restricts the number of States that may join.

protection and non-EU legislations influenced by the EU Directive, is the prohibition of transfer of personal data to countries without adequate data protection legislation. For Nigeria, the low levels of computerisation and absence of privacy advocacy[1177] raise the question whether the regulation of trans-border data flows by way of data protection legislation is a compelling necessity. This question is apt particularly in the light of the numerous developmental and governance deficits that the country is grappling with. Nevertheless, the issue must also be considered in the context of the policy thrust of the country's development strategy - to make Nigeria one of the biggest global economies in the year 2020.[1178]

A fundamental element in achieving the year 2020 objective is to make Nigeria a trade hub not only in the West African sub-region, but also in Africa. The EU presents one of the biggest market *blocs* in international trade and this fact is not lost on Nigeria. If and when Nigeria becomes the continental and regional trade hubs it seeks to be, it is inconceivable that trade between the EU and Nigeria will not involve large volumes of trans-border data flows between the two trade partners. Data protection considerations will arise and must be addressed. Two key questions that the relevant authorities in Nigeria must answer are:

- Whether the EU Directive on data protection requires Nigeria to enact a data protection legislation and if so,
- What model of data protection legislation to adopt?

This chapter will argue that in order for Nigeria to realise its Vision 2020 ambitions, particularly in relation to becoming the international trade hub in Africa, the country must meet the data privacy expectations of its current and potential trade partners abroad. It is necessary for Nigeria to improve its international competitiveness and thereby create opportunities for its businesses to fully participate in international trade. Enacting a data protection law will contribute to the country's competitive

1177 See chap 4 par 6 above.

1178 This policy objective is enunciated in the Vision 2020 policy document. According to the concept paper for the development of Vision 2020, "By 2020 Nigeria will be one of the 20 largest economies in the world able to consolidate its leadership role in Africa and establish itself as a significant player in the global economic and political arena." See *National Planning Commission Nigeria Vision 20:2020* [online].

edge by assuring Nigeria's international business partners that their citizens' personal information will be protected in Nigeria. This in turn will facilitate the smooth transfer of data between, for example, EU member countries that make up a very significant global market block and Nigeria.[1179]

3. THE EU DATA PROTECTION DIRECTIVE AS EMERGENT GLOBAL DATA PROTECTION STANDARD

3.1 The European Union: setting global standards

Having argued that data protection laws have emerged, along with other regulatory regimes, as barriers to the global network market and that the foremost amongst the data protection regimes is the EU Directive 95/46/EC, I will now show how and why the EU Directive emerged as the dominant standard compelling response from diverse non-EU states. The European Union (EU) is a diverse collection of 27 states founded on the ideal of making war impossible, by integrating the economies of its member states to such an extent that armed conflict would be too costly for all sides.[1180] The economic integration between member states of the EU has increased dramatically, and with the addition of new members, the member states have redirected their trade toward the Union and thereby made the EU more self-reliant.[1181] As noted by Heisenberg,[1182] in the 1980s, the EU became a force challenging the dominance of the US in the creation of international regimes.

She argues that by helping to set the parameters within which the US and European firms compete, the EU began to put its own mark on globalization. Thus it was that by the late 1990s, the EU had become the largest single market and its policies had worked to stabilize economic production in the member states. Heisenberg concludes

---

1179 While Article 25 of the EU *Directive* prohibits EU nations from transferring personal data to third countries which do not guarantee adequate protection of such data, it may also be the case that a third country, not a member of the EU, may restrict onward transfers of data to Nigeria as a result of that third country's data protection law which meets the EU standard.

1180 Heisenberg *Can the European Union Control the Agenda of Globalization?* 3 [online].

1181 Ibid.

1182 Ibid.

that the process of deeper European integration and successive enlargements resulted in greater participation in global economic governance and more European policy autonomy.[1183]

Although the EU is not a cohesive, large sovereign state in international affairs, it is one in commercial and economic matters, and has become a powerful actor in international politics and economics. This is because a large market commands more power in the international sphere than many small or medium sized states.[1184] One way in which the EU exercises its economic power is by setting standards. Standards are very important in establishing the parameters of global competition. According to Mattli and Buthe,[1185] as much as 80% of world trade is affected by standards or other technical regulations. Clearly, EU regulations are often characterized by "trading up" to a higher standard rather than "trading down" to a minimum, a fact made possible by the size and attractiveness of the European market.[1186]

Referring to the EU *Data Protection Directive*, Heisenberg argues that by offering alternatives to US proposals or practices, the EU presents citizens of the world a choice of regime that they would not otherwise have had the power to negotiate because of their size.[1187] The European Commission identified data protection as an international issue requiring harmonization in 1990, earlier than the US did, and

---

[1183] Ibid. After the May 1, 2004 enlargement, the EU levelled part of the global playing field when it mustered a total population of over 488 million consumers comprising the 25 member states which compares to the over 288 million population of the US in 2004. On 1st January 2007, the membership increased to 27 countries and the population increased to over 495million people. The EU's population for 2012 is in excess of 501 million people. See EU Eurostat website *EU Population* [online]. The population of the US in July 2012 was over 313 million people. See US Census Bureau website [online].

[1184] See n 1180.

[1185] Mattli and Buthe 2003 (56) *World Politics* (2003) 2.

[1186] In his book *Trading Up: Consumer and Environmental Regulation in a Global Economy* 2, David Vogel analyses the regulatory dimensions of major international and regional trade agreements and treaties such as the EU, GATT, NAFTA, etc, and examined the interaction of trade policy and regulatory policy since both now have international significance. He argues strongly that increased economic interdependence is resulting in stronger consumer and environmental regulation. Trade and trade agreements affect not only the flow of goods among nations but also the movement of regulations across national boundaries. Nations involved in the global trade are increasingly importing and exporting standards as well as goods. See Vogel *Trading Up: Consumer and Environmental Regulation in a Global Economy* 2.

[1187] See n 1180 at 15.

formulated the issue as a "fundamental human right" (thereby making it non-negotiable) as opposed to a commercial one.

Writing elsewhere, Heisenberg and Fandel[1188] argue that the EU *Directive* on data protection has become the *de facto* global standard for data protection and has put data protection in the mainstream of international regulatory regimes. One reason given for the EU ability to project its data protection regime is the threat implicit in the *Directive*, to exclude non-EU countries that fail to comply with the standard set for data protection in the *Directive*.[1189] This threat has been leveraged by the fact of the EU's large internal market which no serious trading partner would care to ignore. Furthermore, the fact that privacy issues have been removed from the WTO's mandate ensures that the *Directive* may not be considered as a non-tariff barrier.[1190]

Other countries have since passed comprehensive privacy legislations to comply with the EU's *Directive*. Even the US could not risk having its data flows cut off; after intense negotiation between the EU and the US Department of Commerce, a compromise[1191] was reached. The EU would allow US corporations to self-regulate their dealings with data from Europe by not treating Europeans' data in a manner incompatible with the *Directive*. According to Heisenberg, although this self-

---

[1188] Heisenberg and Fandel *Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard* 109-129.

[1189] Ibid. See also Shaffer 2000 (25) *Yale J Int'l L*.

[1190] Under the GATS Article XIV, WTO members may adopt and enforce measures relating to services which:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
>
> (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:
>
> (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

[1191] The "Safe Harbor" Agreement came into force on November 30, 2000. The Agreement allows US companies that comply with the 7 principles enunciated in the agreement, to lawfully receive personal data from the EU. Participation in the Safe Harbor Agreement enables US companies that are subject to the EU *Data Protection Directive 95/46/EC* to transfer information lawfully to the United States. Such companies are subject to the *Data Protection Directive* if they:

i. are established in an EU member state, or
ii. use equipment located in Europe to process personal data.

See Kierkegaard 2005 (1) *Shidler JL Com & Tech* 4 [online].

regulatory compromise was flawed in many respects, it did establish unequivocally the Europeans' right and ability to create what amounted to a new global regime in privacy.[1192]

3.2 Is the EU Directive on privacy a violation of WTO's trade rules?

The comprehensive legislative framework that the EU has established by means of the *Data Protection Directive* is aimed at protecting data pertaining to individuals. This regime applies to a wide range of data held by both public and private entities. It imposes significant restrictions on data processing by such entities while granting broad rights to data subjects. It also prescribes a regime of notifications and approvals by enforcement authorities set up by member state governments for many processing operations. The *Directive* prohibits the collection and processing of personal data, subject to exhaustively listed exceptions. The effect is that the law imposes serious restrictions on personal data processing and, where permitted, the data processor bears the burden of proving that the processing is lawful.

For Nigeria and other countries outside of the EU, the most important element of the EU *Directive* is Article 25 which provides:

> The member States shall provide that the transfer to a third country of personal data … may take place only if … the third country in question ensures an adequate level of protection …

The extra-territorial scope of the *Directive* is reflected in the above provision imposing restrictions on transmitting domestic European data abroad; no data can leave Europe unless the transmission goes to some "third country" that "ensures an adequate level of protection." Some of the countries so far recognized by the European Commission are, Argentina, Australia, Canada, Guernsey, Isle of Man, New Zealand, Switzerland 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.[1193]

[1192] See n 1180 at 16-17.

[1193] See the European Commission *Decisions on adequacy* [online].

Data transfers as sale of services fall under the *General Agreement on Trade in Services* (GATS). Under the GATS, member nations are required to accord to one another "most favoured nation" (MFN) treatment whereby one member gives to another "treatment no less favourable than it accords to like services and service providers of any other country."[1194] Article 14 of GATS provides that member nations can adopt measures for the protection of the privacy of individuals and the protection of confidentiality.[1195] Such measures are however subject to the MFN clause of the Agreement. The threat to ban data transfers to third countries without adequate levels of privacy protection has prompted some commentators to hold that such a threat, if carried out, may be in breach of WTO rules. According to Swire and Litan,[1196] the EU data protection regime may be in violation of WTO law, which extends also to e-commerce. This may be so not only with respect to services under the GATS, but also with respect to products under the *General Agreement on Tariffs and Trade* (GATT).[1197] Arguing in support of Swire and Litan's position, Bergkamp[1198] states that the EU privacy laws restrict competition directly and indirectly.

He argues that direct restrictions are caused by the law eliminating privacy protection as an element of competition between suppliers in a market.[1199] This is because EU law, offering a "high level of protection," prescribes the "privacy product" that corporations must offer, and no deviations are permitted. As a result, he says, all corporations offer the same level of privacy protection and any competition as to privacy protection is excluded. He concludes that privacy regulation directly reduces competition in markets for direct marketing services by burdening the sale or licensing of many products and services involving customer data.[1200]

With particular reference to services under the *GATS*, Bergkamp is of the view that

---

1194 *General Agreement on Trade in Services* (GATS) Art 2.

1195 Id Art 14 (c)(ii).

1196 Swire and Litan *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* 145.

1197 Bergkamp 2002 (18) *CLS Rev* 31-47.

1198 Ibid at 39.

1199 Ibid.

1200 Ibid.

EU privacy laws target specifically the clear competitive advantage of US businesses in the area of data management and customer relations management. This is evident in the disparate levels of enforcement of the privacy rules. He sees enforcement under the Safe Harbour arrangement and the model contracts[1201] as more stringent than enforcement of the Directive within the EU.[1202] This disparity, he argues, violates the requirement that US service providers be treated as favourably as EU providers[1203] and that regulation must be applied in a "reasonable" manner.[1204] Thus, if the EU bans the flow of data to the US, but not to other countries with "inadequate" protection regimes, it would most likely violate the GATS most favoured nation clause.[1205]

3.2.1 Exploring the impact of the EU *Directive* on Nigeria in relation to the WTO's trade rules

Since Nigeria does not have a national data protection law, the extra-territorial reach of Article 25 of the EU *Directive* and its potential impact on Nigeria's international trade interests should be examined. At present, there are three Nigerian banks operating through subsidiaries in the United Kingdom and France, members of the EU.[1206] The question arises whether a ban on the transfer of data by those banks and/or other commercial entities to Nigeria constitutes a trade barrier to the supply

---

[1201] Under Article 26 (4) of *Directive 95/46/EC*, the European Commission is empowered to decide that certain standard contractual clauses provide sufficient safeguards in respect of the privacy and fundamental rights and freedoms of individuals, in line with Article 26 92) thereby ensuring that personal data can flow from a member state of the EU to a third country without an adequate level of data protection. See European Commission *Decision 2001/497/EC of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Under Directive 95/46/EC*, 2001 O.J. (L 181) 19-31.

[1202] See n 1197 at 39. Under the Safe Harbor regime, in addition to the US Federal Trade Commission, a special Commission of EU data protection Commissioners supervises compliance with the regime and handles complaints. The EU model data transfer contract provides for enforcement under civil law by data subjects as third party beneficiaries.

[1203] *General Agreement on Trade in Services* (GATS) Article XVII.

[1204] Article VI (GATS).

[1205] Article II (GATS). However, contrary to Bergkamp's argument, art 25 of Directive *95/46/EC* applies to all countries without adequate levels of protection for personal data.

[1206] The parent Nigerian banks are First Bank of Nigeria Plc, Zenith Bank Plc and GTBank Plc. Other banks are at advanced stages of their preparations to launch in the EU, while some Nigerian companies, including financial institutions are already quoted on the London Stock Exchange.

of services by those companies in Europe?

Under the most-favored nation clause,[1207] the EU cannot accord less favorable treatment to Nigerian services and service providers than to those of any other WTO members. If the ban on transfer of data to Nigeria applies equally to all other countries adjudged by the EU not to have adequate data protection, it would be hard to prove discrimination since the ban would then be an indirect consequence of the operation of the Directive affecting other countries as well.

Although no formal finding has been made by the EU regarding adequacy of privacy protection in Nigeria, a relevant question to ask is whether the country can complain that the threat to ban data transfers to Nigeria, on the ground of inadequate level of data protection, violates international trade rules. This question of course assumes that there is a measure of protection already in place. The question is particularly pertinent in the light of Nigeria's desire to harness the benefits of trade in services and become a hub for outsourcing services.

Because economic progress and trade competitiveness depend very much on the free flow of information, Nigeria cannot afford to be shut out of the flow because of the unavailability or inadequacy of its data protection regime. As observed by Reidenberg,[1208] flows of information and access to global information networks depend increasingly on emerging fair information practice rules and, specifically, the protection of personal information or information about individuals. The regulation of information practices will determine the availability of data and the possibilities for interconnection of networks.

Shaffer[1209] argues that the EU's response to the effect of its Directive on cross-border transfer of personal data might be that it is an indirect effect; such an indirect effect on the provision of services in the EU could not be covered under GATS because ultimately all measures have indirect effects. However, it is arguable that a ban on data transfer to Nigeria has foreseeable effects on the provision of services by

[1207] See GATS art II.

[1208] Reidenberg 1993 (6) *Harv J L & Tech* 288.

[1209] Shaffer 2000 (25) *Yale J Int'l L* at 50.

Nigerian-owned service providers in the EU market, even if such effects are indirect. The argument notwithstanding, it will be difficult to sustain a case against the EU since by its operation, Article 25 of the EU *Directive* is known to apply to all third countries outside the EU.

According to Shaffer, an objection to the EU's Directive on account of Article 25 thereof, might not succeed for three reasons:

- The *Directive* applies equally to transfers to all countries and thus should not violate the GATS most-favoured nations' clause. It applies equally to EU-owned and registered companies and foreign-owned and registered companies and thus should not violate the GATS national treatment clause. So long as the EU does not clearly discriminate against the U.S. or U.S. service providers in its application of the *Directive*, the United States would likely not prevail.[1210]
- The GATS' general exception clause, Article XIV, explicitly authorises WTO members to restrict commerce in order to protect *inter alia* "the privacy of individuals." Since the privacy interests of EU residents are directly at stake, it is unlikely that a WTO panel would find the Directive's content to be "unreasonable."[1211]
- A WTO panel will be wary of engaging in a delicate balancing of trade and privacy interests, particularly since the privacy of residents within the EU, as opposed to outside the EU, are directly at stake. Under media scrutiny, WTO dispute settlement panels would prefer to refrain from engaging in a close balancing of competing trade and privacy interests, and rather review the process by which the EU takes account of foreign privacy protections. This is the approach recently taken by the WTO Appellate Body in an analogous case.[1212]

In the end, rather than complain about the EU *Directive*, a complaint that may not

---

[1210] Ibid.

[1211] Ibid.

[1212] Id at 51.

be sustainable before a WTO dispute settlement panel, it is suggested that a better option is to study and understand the EU's process for assessing adequacy of privacy protection and then adopt an appropriate data protection model that will meet the EU's requirements.

3.3 The EU process for assessing adequacy of data protection in a third country

The European Commission is required to make a determination of the adequacy of data protection in a third country with the help of a Committee and a Working Party. The Committee, which is set up under Article 31 of the *Directive* on privacy, is made up of Member State officials and every Member State is represented. Its mandate is to advise the Commission on decisions concerning the adequacy of the protection of individuals with regard to the processing of personal data for the purpose of transferring same to non-EU countries.

The Working Party is established under Article 29 and is composed of the data protection commissioners, or independent supervisory authorities, of all the Member States. Its mandate is wider than that of the Committee as it plays a crucial role in helping the Commission ensure even application of the Directive's requirements across the EU. Under Article 25(6), the Commission has the power to determine whether a non-EU country ensures an adequate level of protection by reason either of its domestic law or of the international commitments it has entered into. Upon the advice of the Working Party, the Commission has recognised that an adequate level of protection could also be provided by sector specific legislation or effective self-regulatory schemes (for example, schemes whose enforcement is underpinned by law).

> The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms

and rights of individuals.[1213]

The *Directive* requires that a determination of the adequacy of a third country's data protection laws should be in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Consequently, some of the particular considerations that shall be taken into account in making a determination as to adequacy are:[1214]

(a) The nature of the data
(b) The purpose and duration of the proposed processing operation or operations
(c) The country of origin and the country of final destination
(d) The rules of law, general and sectoral, in force in the third country in question
(e) The professional rules and security measures which are complied with in that country

Where a data privacy authority in a member state makes a finding that a third country lacks adequate protections, such authority is required to report such a finding to the Commission.[1215] In practice however, no member state has made any adequacy determination;[1216] the Commission has largely been responsible for making determinations as to adequacy.[1217]

The Working Party set out a complete framework of the substantive requirements that a given data protection regime must meet.[1218] The document essentially encompasses the core data protection principles distilled from international documents such as the Council of Europe *Convention No 108* of 1981,[1219] the OECD

1213 Art 25 (6) of *Directive 95/46/EC*.

1214 Art 25 (2).

1215 Art 25 (3).

1216 See Bignami 2005 (26) *Mich J Intl L* 832.

1217 EU Commission *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive.* DG XV D/5025/98WP 12 (1998).

1218 Ibid.

1219 Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of*

Guidelines of 1980[1220] and the UN *Guidelines* of 1990.[1221]

Although the *Directive* contains no specific definition of "adequate level of data protection", it provides at least five fundamental criteria of consideration of data privacy management in a third country. According to Zinser, the five criteria for consideration are:

(a) The lawfulness of the processing of personal data
(b) The special protection of sensitive data
(c) The rights of the data subjects
(d) The security of the actual processing of data
(e) The existence of control and enforcement measures.[1222]

As noted by the Working Party,[1223] European countries have historically tended to embody data protection rules in laws that make provisions for sanctioning non-compliance and also for individuals to be able to obtain redress when their privacy rights are breached.[1224] Such legislation usually makes provision for the establishment of supervisory authorities that perform monitoring and complaint investigation functions.

The Working Party however, concedes that outside of Europe, it is not common to find such procedural mechanisms for enforcing compliance with data protection rules. Nevertheless, the Working Party maintains that "any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application."[1225] Essentially therefore, a determination of the adequacy of data protection in a third country will require examination of the country's regime of statutes, rules and regulations governing data/privacy protection. The regulatory regime is judged in the light of

---

Personal Data CETS No. 108 (1981) which entered into force on 1 October 1985.

1220 OECD *Guidelines on the Protection of Privacy and Transborder Flows.*

1221 UN *Guidelines for the Regulation of Computerized Personal Data Files* (1990).

1222 Zinser 2003 (21) J *Marshall J Computer & Info L* 559.

1223 See n 1217.

1224 See n 1217 at 5.

1225 Ibid.

content principles that specify minimum requirements for the protection prescribed in the regime for it to be judged as adequate. The Working Party has identified nine content principles:

(a) The purpose limitation principle
(b) The data quality and proportionality principle
(c) The transparency principle
(d) The security principle
(e) The rights of access, rectification and opposition
(f) Restrictions on onward transfers
(g) Special handling of sensitive data
(h) Possibility to 'opt-out' from direct marketing
(i) Special rules for automated individual decision making.[1226]

The supervisory structure for enforcing the regulatory regime is judged by Three enforcement objectives are identified:

(a) to deliver a good level of compliance with the rules;
(b) to help data subjects in the exercise of their rights; and
(d) to provide appropriate redress for the injured party where the rules are not complied with.[1227]

3.4 Assessing the adequacy level of data protection in Nigeria

While there is at present no omnibus privacy or data protection law in Nigeria, personal data are protected to some extent by a number of statutes, each of limited scope and application. The need for more comprehensive data protection is acknowledged in the country's IT Policy. The Policy recognises the need to "promote legislation (Bills and Acts) for the protection of on-line business transactions, privacy and security" and to "enhance freedom and access to digital information at all levels while protecting personal privacy".[1228] No data protection legislation has so far been

[1226] See n 1217 at 6-7.

[1227] See n 1217 at 7.

[1228] NITDA *Nigerian National Policy for Information Technology (IT)*.

passed. The earliest attempt at protecting personal information was a private member's Bill which was presented in the House of Representatives (lower chamber of the National Assembly) for an Act to provide for the establishment of the Cyber Security and Information Protection Agency. The proposed agency, if established by the proposed Act, would have been responsible for securing computer systems and networks in Nigeria. It would also have had to liaise with the relevant law enforcement agencies for the enforcement of cyber-crime laws and other related matters.[1229]

Furthermore, the agency was proposed to investigate and prosecute individuals and corporate organisations involved in computer and Internet-related criminal activities. It would have been responsible for the registration and regulation of network service providers in Nigeria and the creation of public awareness on the nature and forms of cybercrimes.

A careful reading of the proposed legislation shows that its emphasis is cybercrime and not data protection. The nearest it comes to dealing with data protection is the section dealing with identity theft.[1230] The Bill proposes that anyone who assumes the identify of another person with the intention to deceive or defraud "commits an offence and shall be liable on conviction to a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment".[1231] The Bill, if passed into law, will not meet the specific demands for data protection legislation in Nigeria.[1232] As needful as cyber-crime legislations are in curbing the excesses associated with the digital age and Internet usage, they cannot adequately address the nuanced environment of personal information security. Such legislations focus on individuals perpetrating the crimes whereas personal data

[1229] HB 154 Cyber Security and Data Protection Agency (Establishment etc) Bill.

[1230] Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. See US Department of Justice *Identity Theft and Identity Fraud* [online].

[1231] See n 1229 at s 14.

[1232] HB 154 Cyber Security and Data Protection Agency (Establishment etc) Bill was introduced in 2008 and sponsored by Hon. Etim Bassey of the House of Representatives. Another Bill, the Electronic Fraud Prohibition Bill, 2008 (SB. 185) was sponsored by Senator Ayo Arise in the Senate. Neither of the two Bills was passed by the National Assembly by the time the legislative year ended in May 2011.

breaches very often involve corporate and state entities that are removed from the scope of the laws.

Furthermore, cyber-crime legislation seldom provides avenues for compensation to the victims of the crime. Whereas the law, as in the proposed Bill above, prescribes the payment of fines, such fines are not directed to the benefit of the victim of the crime of identity theft.[1233] Data protection laws on the other hand, are invariably derived from globally accepted data protection principles,[1234] and such laws usually make provisions for appropriate redress for the injured party where the laws are not complied with.[1235]

Interestingly, one of the conditions stipulated by Nigeria under its schedule of specific commitments under the *GATS* in regard to financial services is that: "[t]he transfer of information containing personal data, bank secret, securities secret and/or business secret is not allowed."[1236] This commitment has not yet crystallised into an enforceable statutory provision. The EU *Directive* is specific on the requirements for the transfer of data. Under the *Directive*, the third country should provide an adequate level of protection for personal data of the citizens of EU member states. It envisages a framework of protection for data that enters into the third country for processing, storage and/or re-transmission, and not a blanket ban on the outward flow of data from the country. Since 2010, there have been renewed efforts to draft a data protection law for Nigeria. The efforts have not yet crystallised into a substantive data protection law. However, when the efforts do result in a framework for data protection in Nigeria, the adequacy level of such framework will

---

1233 Take eg, the case of phishing. The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication. When the victim of a phishing attack responds, in ignorance, to the bait presented by the supposedly official electronic communication, the result is very often loss of money. The perpetrator usually seeks to persuade the victim to disclose confidential information on a website that appears to be the website of the victims bank and then uses the disclosed personal information to gain access to the account of the victim. For more information see the website of the Anti-phishing Working Group [online]; see also Jakobsson *Human Factor in Phishing* [online].

1234 See n 1220.

1235 See n 1221.

1236 See World Trade Organisation *Nigeria: Schedule of Specific Commitments* 2.

be assessed in the light of the content and enforcement principles outlined in the Working Party's working document referred to previously.[1237]

3.4.1 Assessing statutory and common law protection of privacy in Nigeria in the light of Directive 95/46/EC

In chapter 4, a general overview of the constitutional and statutory protection of privacy in Nigeria was undertaken.[1238] It was asserted that the judicial enforcement of the constitutional right to privacy has been minimal. The dearth of case law in this area of Nigeria's jurisprudence points to a weakness in the protection of privacy generally. The point was also made, that the statutory protection of privacy is more concerned with securing the confidentiality of information collected by the government and its agencies. They do not address private sector collection and processing of personal information. With particular reference to information privacy, it was asserted that the reference to correspondence, telephone conversations and telegraphic communications indicates a clear intention to protect information privacy. This intention is however, not borne out by a robust case law of information privacy protection.

3.5 Adequacy of the supervisory structure for enforcing the protection of data privacy

The EU *Data Protection Directive* also requires, in the evaluation of the data protection adequacy level in a third country, the existence of a supervisory structure for enforcing the protection of data privacy. The European model of data protection regimes is characterized by two main features: the regimes are embodied in written law and are enforced by national data protection agencies. These national data protection agencies complement and strengthen the legal regime by informing and educating the public about their rights in relation to their personal data and by providing readily identifiable processes by which complaints from the public may be

[1237] See n 1217.

[1238] See chapter 4 par 6.

investigated and settled, either within or outside the judicial system. By their activities, they generally ensure that data protection laws are enforced.

The Article 29 Working Party has discussed its methods of evaluation in a number of adopted documents;[1239] the most comprehensive and indeed, the latest of these documents is WP 12. It describes a complete framework of substantive requirements that a given data protection regime must meet.

In evaluating the level of adequacy of data protection, particularly with regard to the supervisory and enforcement infrastructure, the Working Party has provided a set of criteria by which the effectiveness of such a data protection implementation system can be measured.[1240] These criteria are:

(a) The "ability of the system to deliver a good level of compliance with the rules".[1241]

(b) The regulatory system must be able to give sufficient "support and help to individual data subjects in the exercise of their rights".[1242]

(c) The system must be able to provide appropriate redress for the injured

---

[1239] The main documents are:
1. Discussion Document: *First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy* ("WP 4");
2. Working Document: *Judging Industry Self-Regulation: When does it make a meaningful contribution to the level of data protection in a third country?* ("WP 7");
3. Working Document: *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive* ("WP 12").

[1240] Ibid.

[1241] A system with such ability is characterised by the following factors:

- A high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them;
- The existence of effective and dissuasive sanctions;
- The existence of systems for direct verification by supervisory authorities, auditors or independent data protection officials. See n 1217 at 7.

[1242] Relevant factors to consider include:

- A rapid and effective means of redress for the individual;
- The cost of redress (for the individual) should not be prohibitive;
- A complaints referral mechanism. The individual should know who to contact for the purpose of a data challenge. This presumes that the data subject has become aware of the transfer of and the subsequent reuse or disclosure of those data;
- Some form of institutional mechanism for the independent investigation of complaints. This is seen as preferable to other complaints options;
- Mutual recognition or assistance between supervisory authorities to facilitate investigations, where data have been transferred to a third country.
- Dispute resolution mechanisms which are timely and readily accessible to the data subject, and which can be tailored to the particular characteristics of privacy disputes.

party where the rules are not complied with.[1243]

3.5.1 Evaluating the effectiveness of Nigeria's data protection system against the EU's assessment criteria

3.5.1.1 The "ability of the system to deliver a good level of compliance with the rules"

The Working Party acknowledges that no system can guarantee 100% compliance, but that some are better than others; it is also aware that a "good level of compliance" may be subjective and hard to quantify. In the case of Nigeria, it is safe to say that generally, the level of awareness by consumers, of the statutes and common law remedies that could potentially protect some aspects of their privacy and personal data is very low. This low awareness also accounts for the paucity in Nigerian case law on privacy protection. The same can also be said of those who may be regarded as data controllers, particularly those employed by federal, state and local governments, who engage in data collection and processing.

Public policy in Nigeria acknowledges the constitutional right to privacy. For example, the Central Bank of Nigeria issued a guideline on e-banking that reiterates the need for banks to protect the privacy of customer's data by ensuring that:

- Customer's personal data are used for the purpose for which they are compiled,
- consent of the customer must be sought before the data is used,
- data user may request, free of cost, the blocking or rectification of inaccurate data or may enforce a remedy against a breach of confidentiality,
- processing of children's data must have the consent of the parents and there must be verification via regular mail,
- strict criminal and pecuniary sanctions are imposed in the event of

[1243] The third criterion requires:

- The right to have a complaint adjudicated by an independent arbiter;
- Some form of remedy for the data subject, such as compensation and/or injunctive or declaratory orders;
- The availability of appropriate dispute resolution mechanisms, and for these arrangements to be prescribed at the time of contract formation.

default.[1244]

Arising from the above guideline, most Nigerian banks with Internet presence have formulated privacy policies that notify customers of the fact and circumstances under which their personal data are collected and disclosed by the banks either online or offline.[1245] Apart from the banking industry however, the other organized sectors of the economy operate without privacy policies or voluntary codes of conduct and even where such codes exist, they are not readily accessible to the public.

3.5.1.2 The regulatory system must be able to give sufficient "support and help to individual data subjects in the exercise of their rights"

The minimal data protection rules embedded in the statutes and common law torts in Nigeria come with their associated legal processes and remedies. Judicial review of alleged privacy breaches is available and even though such cases are rare, the review processes are reasonably independent and their outcomes enforceable. However, because the processes are cumbersome, recourse to litigation is a slow and expensive way to resolve data protection complaints if they arise.

3.5.1.3 The system must be able to provide appropriate redress for the injured party where the rules are not complied with

A fundamental weakness in the Nigerian system is the lack of information concerning the exact content of data protection rules where such are available. Data protection rules are generally absent, or where available as in the banking industry, it is difficult for a data subject to seek redress or make a claim.

The Central Bank directive on data protection in the banking industry only provides

---

[1244] Central Bank of Nigeria *Guidelines on Electronic Banking* 10 [online].

[1245] A careful sampling of these websites will show that there is no consistency in the policies; each bank adopts the policy that it deems fit for its business. Moreover, some of the privacy policies are characterized by exceptions which allow the banks to transfer personal data collected to subsidiaries without recourse to the individual involved. See eg, Standard Chartered Bank Plc website [online]; some of the websites, like the forgoing, use cookies, while others claim not to, such as Access Bank Plc website [online]. First City Monument bank acknowledges the use of cookies and even provides a link for customers who wish to disable the use of cookies. See their website [online].

for a system where the bankers, as data controllers, implement the system. Aggrieved customers do not know who to complain to in the event of a breach of their privacy rights. There is no provision for the payment of compensation and no help or support procedure is available to the customer to complain and seek redress directly from the data controllers.

3.6 Conclusions drawn from the assessment of the adequacy of data protection in Nigeria

The inescapable conclusion, arising from the foregoing assessment, is that the supervisory structure for enforcing data protection rights in Nigeria is virtually non-existent. Such structure as may be available today is fragmented, incoherent and therefore inadequate to address the multi-faceted issues affecting the collection and processing of personal data in the 21st century. The fact that the system is fragmented also makes monitoring and auditing by the relevant state authorities difficult.

In an era of increasing globalization, e-commerce and outsourcing, Nigeria's inability to assure its international business partners that their customers' personal information will be protected, is a potential impediment to trade. This is a significant risk for Nigerians and Nigerian businesses that wish to enter into international arrangements. Currently, the only option is for those companies to enter into special contractual arrangements for privacy protection, thereby resulting in additional transaction costs.

A data protection law in Nigeria, while essentially responding to European Union requirements, will also tell an important message about how Nigeria is willing to deal with other nations. It will show that if Nigeria wants to have trade relationships with other countries, it is prepared to abide by the standards dictating access to and interaction in the global market network by having data protection provisions that are up to global standards and are accepted by those countries as providing sufficient protection. In answer therefore to the question whether Nigeria needs to respond to the data protection requirements of the EU *Directive*, the foregoing analysis leads to a compelling conclusion that Nigeria needs to respond by enacting a data protection legislation that meets international standards.

4. DEVELOPING A NIGERIAN DATA PROTECTION FRAMEWORK

4.1 Law reform as vehicle for sustainable economic and social development.

> A modernizing nation's economic prosperity requires at least a modest legal infrastructure centered on the protection of property and contract rights. The essential legal reform required to create that infrastructure may be the adoption of a system of relatively precise legal rules, as distinct from more open-ended standards or a heavy investment in upgrading the nations judiciary.[1246]

As Posner asserts above, it is desirable, for a country's prosperity, for it to have at the minimum, a legal system that protects property and contract rights.[1247] Salacuse[1248] observed however, that development strategies in the developing countries during the late 1950s and 1960s saw a shift from private ordering to public ordering of economic and social activities. According to him, two development models, Development Model 1[1249] and Development Model 2,[1250] have characterised the development strategies of developing countries in the Third World.

1246 Posner 1998 (13) *World Bank Res Obs* 1.

1247 Western developed nations recognised this concept and gave premium to the private ordering of economic and social activity. English common law, and to a great extent the Continental Civil law codes, have for long reflected the shift from status to contract beginning from the 19th century when individual's rights were determined more by their private contractual arrangements than their status in society. See Seidman 1966 *Wis L Rev* 999.

1248 Salacuse 1999 (33) *Int La Int Lawyer wyer* 875.

1249 Ibid. Development Model 1 was characterised by a fundamental belief that governments had the primary responsibility for bringing about economic development. The model had 4 basic elements: 1. Public ordering and state planning of the economy and society; 2. Reliance on state enterprises as economic actors; 3. Restriction and regulation of private enterprise; and 4. Limitation and control of the country's economic relations with the outside world. Under the model, governments, through planning ministries, departments and institutes prepared development plans to guide and direct the various activities that would lead to development. The result was increased regulation and restriction of the private sector.

1250 See n 1248 at 882-889. Development Model 2 is characterised by: 1. Reliance on Markets and private ordering, 2. Privatisation, 3. Deregulation and 4. Opening up of the economies. Under this model, state planning of the economy is de-emphasised thereby allowing market forces free play in determining production and prices. Decisions on investments, commodity prices and credit allocation are increasingly made by private actors in the market.

The choice of Model 1 not only affected the economies of the countries but also impacted their legal systems. By emphasising state planning and heavy regulation, public law was greatly relied upon to achieve the set objectives while private law was hardly developed nor played a major role in the development process.[1251] Courts had a limited role in the development of the laws shaped by the Development Model 1. In many respects, many governments openly and actively sought to weaken the independence of the judiciary by either disobeying court orders or promulgating new laws to nullify unfavourable court decisions.[1252]

By the mid-1980s however, Development Model 1 was out of favour principally because the pervasive regulatory systems required by the Model eventually came to be seen as obstacles to economic development and also because of the imposition of new requirements by international financial institutions and aid donor agencies. [1253] There is now an on-going process of shifting from Model 1 to 2 with the necessary modifications the shift entails.[1254]

The shift has also meant a return to private ordering of economic activity. There is increased freedom of contract; the form and substance of transactions in the

---

[1251] According to Salacuse "During the era of Development Model 1, a plethora of new laws and regulations mushroomed where none had existed before. Public enterprise laws, foreign investment codes, currency control regulations, to name just a few, filled the law books, and became the fundamental preoccupation not only of government officials, but of lawyers and legal scholars as well. This new public law, not the commercial code, became the basic law of economic and business activity in the Third World." (p 881).

[1252] For example, the Nigerian Military Government enacted the Federal Military Government (Supremacy and Enforcement of Powers) Decree, 1970 which provided: "Any decision, whether made before or after the commencement of this Decree, by any court of law in the exercise or purported exercise of any powers under the Constitution…which has purported to declare or shall hereafter purport to declare the invalidity of an Decree or Edict… or the incompetence of any of the governments in the Federation to make the same is or shall be null and void and of no effect whatsoever as from the date of the making thereof."

[1253] See n 1248 at 885-886. The International Monetary Fund (IMF) and the World Bank have in the recent past been vilified in Third World countries because of their so-called "conditionalities", the IMF more so. Another reason for the failure of Model 1 was the successful example of the Asian 'Tigers' that had avoided some of the elements of the Model such as restrictions on foreign capital flow and private enterprise.

[1254] See n 1248. According to Salacuse, "The shift from Development Model 1 to Development Model 2 has important implications for the Third World legal systems. First, the idea that law is a tool for social engineering and that legislation can bring about sweeping changes in human behaviour is much less prevalent now than it was thirty years ago… Rather than relying on coercive pressure to bring about change, as was so common in early days of the development era, the law now tends to employ incentives to affect behaviour." (886-887).

marketplace is less mandated by government regulations.[1255] Also, the shift from the closed economies of Model 1 to the openness of Model 2 has resulted in greater participation by developing countries in international organisations such as the World Trade Organisation (WTO) and World Intellectual Property Organization (WIPO) to mention a few.

This greater interaction with the global market network and its compelling regulatory regimes places an overbearing burden on developing countries by requiring them to adapt or upgrade their internal regulatory systems to meet international standards. Only a reasonably well functioning legal system at the national level can ensure that local standards meet international benchmarks.

4.2 Establishing a regulatory framework for the digital marketplace

The complexities of the global market network place an enormous burden on Nigeria to establish a regulatory framework in order to operate effectively in the digital marketplace. The fact that a reasonably well functioning legal system is a necessary condition for a country's prosperity cannot be denied. When law is weak or the legal system is in disarray, the enforcement of property, contract and human rights is weak or frequently depends on the threat or the actuality of violence and in the long run adds extra costs to the cost of business transactions.[1256]

From the information privacy perspective, the most important rationale for establishing a regulatory framework for the digital marketplace in Nigeria is the need to strike the right balance between the protection of the individual's right to his/her personal and informational privacy and the need to enhance governance, national development and other service delivery capacities as well as facilitating electronic and international commerce through access to personal information. This can best be

[1255] While regulation under the old model was aimed at directing transactions in particular ways adjudged by the government as needful, the role under the new model is that of protection of participants in the marketplace from fraud, coercion and abuse by other participants.

[1256] In Nigeria, frustration and the loss of confidence in the state to protect and enforce rights essentially led to the emergence of dangerous parallel justice systems in some parts of the country. The 'Bakassi Boys,' Oodua People's Congress (OPC) and the like are examples. During the period under military rule, it was common for persons frustrated by the long process of judicial redress to employ the services of military men to settle scores or effect the performance of obligations and perhaps avoidance of same.

secured through strengthening regulatory and institutional frameworks and having a robust judicial system. Acknowledging the importance of sound judicial systems to good governance and economic growth, the World Bank and several other donor organizations have funded judicial reform projects in several developing countries.[1257]

Nigeria's legal and judicial system is made up largely of received colonial statutory and English common laws, the bulk of which were enacted in the 19th century. Its commercial laws for example, are perhaps some of the least developed areas of post-independence Nigerian law. This is all the more glaring when one considers the considerable changes that have since been witnessed in national and international commerce. For example, the basic commercial law is derived from 19th century English statutory and common law, such as the Sale of Goods Act, 1893. When this law was enacted, the most advanced means of communications were the telephone and telegraph that were not even at the time universally available as today. In effect, the bulk of Nigeria's statutory laws inherited at independence and still extant, were intended to regulate and facilitate paper-based transactions, and where necessary, punish criminal conducts that were committed in a physical environment. Today's marketplace is increasingly going digital and cyberspace denotes today's business environment.

The movement of information over the Internet for the purpose of trading and communication presents new and sophisticated threats for both sender and receiver of such information. Legal, procedural and technical means of ensuring the security of data are imperative if the use of the Internet and e-commerce must flourish in Nigeria. It is needful for the government to play a leading role in fashioning out a legal and regulatory framework for the use of the Internet and e-commerce. This will be accomplished by the enactment of appropriate legislation and regulations to **e**ncourage user trust in the system.[1258]

1257 Messick 1999 (14) *WBRO* 1-8.

1258 In Nigeria, majority of sales take place in the open local markets, which are largely controlled by age-old customs and practices. The norm usually is that individual buyers and sellers openly strike bargains in the course of physical examination of the goods, following which payment is made and the goods delivered simultaneously. A lot of personal goodwill goes into buying and selling and the effect of this and other peculiarities of the Nigerian buyer and seller make e-commerce not very attractive to the average Nigerian consumer. Any e-commerce marketing strategy therefore that does not take cognisance of some of these

4.3 Why Nigeria should have a data protection law

4.3.1 To regulate the collection, processing, storage and use of personal information

Key sectors of the Nigerian economy are witnessing a continuing migration of critical data to the Internet. These sectors, such as oil and gas, financial services and telecommunications, are critical sectors of the country's national economic and security interests. Computer systems and networks running those sectors constitute the critical information infrastructure; their impairment would have a negative impact on the overall economy and well-being of Nigerian citizens. In addition to the growing reliance on ICTs and the Internet, there is a growing mass of customers subscribing to online services offered both by the financial and telecommunications companies in Nigeria. This proliferation of business activities in relation to customer information demands that customers' personal data are protected.

The collection of personal information in Nigeria has historically been dictated by the requirements of extant legislations and has usually been intended to achieve service delivery objectives as stipulated in the relevant statutes. For example, a Nigerian citizen or legal resident who desires to drive a vehicle within the territory of Nigeria is required to obtain a driver's licence from the Federal Road Safety Commission. The intending driver is required to disclose certain personal information in the application for driver's licence.[1259] While the federal and state governments are the foremost collectors of personal information, the banks and telecommunication service providers are significant personal information collectors in the private sector. The bulk of information collected, whether by the government or private sector entities, are usually given for the purpose of obtaining specific public services or services from the private sector service providers.

---

quaint eccentricities of the Nigerian market place may fail to carry the consumers. With this mind-set, it is most essential for there to be a well-regulated environment that will reassure the average consumer to entrust his personal information and money to faceless entrepreneurs.

[1259] See s 11 of Federal Road Safety Commission Act. Other statute-related personal information collection agencies of government are: the Independent National Electoral Commission (INEC) for the issuance of voter's cards; the National Health Insurance Scheme (NHIS) for health insurance card; the Nigerian Immigration Service, for passports and visas; the National Identity Management Commission (NIMC) for national ID card and the Federal Inland Revenue Service (FIRS) for tax identification number and tax related transactions.

With the phenomenal success recorded by the mobile telecommunications industry in Nigeria since the introduction of mobile telephony in February 2001,[1260] operators in the industry, for example, have in the last nine years accumulated an abundant archive of text messages and other personal information sent by their customers without any legal guide as to how the information should be used. Banks and financial institutions for their part have also accumulated a lot of personal information about their customers. Even though some measure of direction has been given by the Central Bank on how to deal with customers personal data,[1261] the reality is that no one can say with any certainty that there are no breaches of customers' personal data.

Because there is no data protection law and therefore no requirement of authorization before use, it is safe to say that personal data in Nigeria are routinely abused. If personal data can be sold or used without the data owners' permission in countries where data protection laws are extant, it is better imagined what happens in an unregulated environment such as Nigeria. A data protection law that will guarantee the protection of collected personal information privacy is therefore needed.

4.3.2 To fulfil Nigeria's bilateral and multilateral treaty/convention obligations

Nigeria's bilateral and multilateral obligations arising from conventions or other treaties it has signed obligate it to update its legal system to meet global standards and address the realities of the Internet-empowered 21st century. For example, Article 39 of the *TRIPS Agreement*[1262] makes provision for the protection of personal

---

[1260] According to the NCC, mobile phone subscription has grown from 422,000 in 2001 to about 119,356,665 users at the end of April 2013. See NCC website [online].

[1261] See n 1244.

[1262] World Trade Organisation *Agreement on Trade-Related Aspects of Intellectual Property Rights*. (TRIPS). The TRIPS Agreement is Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15th April 1994. Article 39 provides:

> 1 In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.

data submitted to governments or governmental agencies against disclosure without the consent of the owner of the information. The article clearly envisages a national data protection regime in WTO member states that will protect personal data as well as pharmaceutical, agrochemical and traditional medicine-related data against disclosure and unfair commercial use by third parties.[1263] There is no provision in the law that established the National Agency for Food and Drug Administration and Control (NAFDAC),[1264] the regulatory agency for foods, drugs, cosmetics, chemicals and medical devices, for the protection of personal data submitted to it in the course of its regulatory functions.

Another example of treaty obligation requiring Nigeria to enact a data protection law is the ECOWAS Treaty under which the Supplementary Act A/SA. 1/01/10 on

---

2 Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by or used by others without their consent in a manner contrary to honest commercial practices so long as such information:
   a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
   b) has commercial value because it is secret; and
   c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it a secret.

3 Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

[1263] The protection conferred on data submitted for the marketing approval of the product in accordance with Article 39.3 of the TRIPS Agreement has been a problematic issue in some countries. While Article 39.3 obliges WTO Member States to protect clinical data made for registration purposes against "acts of unfair competition", some interested parties have argued that Article 39.3 requires the introduction of "data exclusivity" provisions as operated in the EU or USA. Data exclusivity prevents the regulatory authority from making reference to the original clinical data for a set period, thereby creating a form of market exclusivity during which no authorisation of generic medicines may take place. This debate about data protection and data exclusivity derives largely from the differing interpretations of what the agreement on *Trade-Related Aspects of Intellectual Property Rights* (TRIPS) says on the subject. The protection of data submitted for marketing approval should be granted under the discipline of "unfair competition" and not market protection. See generally Clift "Data Protection and Data Exclusivity in Pharmaceuticals and Agrochemicals" 431- 433. See also the EGA Position Paper *TRIPS Article 39.3 does not Require Data Exclusivity Provisions* [online].

[1264] The National Agency for Food and Drug Administration and Control (NAFDAC) was established by Decree 15 of 1993 with the mandate to regulate and control quality standards for Foods, Drugs, Cosmetics, Medical Devices, Chemicals, Detergents and packaged water imported, manufactured locally and distributed in Nigeria.

Personal Data Protection within ECOWAS was adopted in 2010. The Act requires Nigeria and all other members of the ECOWAS to adopt the data protection law enacted by the regional body or enact their own laws in harmony with the ECOWAS law. This requirement was discussed in the previous chapter.[1265]

4.3.3 To avoid EU sanction against data transfers to Nigeria

The EU nations remain a significant block of Nigeria's trading partners and bearing in mind the stringent requirements of the EU *Directive,* there is a need for legislative intervention to protect private data. It is important that Nigeria's privacy laws keep pace with international norms and not hinder international trading opportunities. It is equally important that Nigeria, although a developing country, is able to stay relevant, by continuing to play on the international stage. This will be effective only if its systems and protections have the same integrity as those in other countries, particularly its larger trading partners. In an era of increasing globalisation and e-commerce, Nigeria's inability to give this assurance is a potential impediment to trade which the country can ill afford.

4.3.4 To provide an effective regulatory and enforcement regime for the protection of information privacy in Nigeria

Another reason Nigeria needs to enact a data protection law is that data protection law is necessary not only to protect the privacy rights of Nigerian citizens, but also to hold all collectors and users of personal data, including cyber criminals, responsible for their wrongful dealings with private data. A well-crafted data protection law will protect the interests of not only Nigerians, but every person resident in Nigeria. Contrary to what many critics of information privacy have suggested, data protection is not about keeping personal information secret, but rather, it is about creating a trusted framework for the collection, exchange and use of personal data in commercial and governmental establishments. A data protection law in Nigeria will regulate and thereby facilitate the use of personal data by all operators in the marketplace in an environment that will greatly reduce the incidence of and potential for abuse.

[1265] See chp 6 par 6.5.6 above.

Furthermore, a data protection regime will impose discipline over a new breed of Nigerian information technology professionals who are yet to be regulated by any enforceable code of ethical behaviour in relation to their handling of personal data. These professionals have the potential to wield tremendous power over consumers by virtue of their control over personal data. The reliance on their good behaviour, in the absence of a data protection law in Nigeria, is unjustifiable in the light of the global perception of Nigeria as a major source of Internet-related fraud.[1266] Individuals do not have legal rights to check that their records in computer databases are correct and up to-date. Indeed, Nigerians do not have the right to access computerised records kept by the government and private companies about them. In the event that such data is found to be incorrect, there is no recognised channel for complaint and correction. Unethical computer users who intentionally misuse computerised personal data are not directly liable for a criminal offence. The absence of a data protection regime is a significant business and social deficit in Nigeria.

4.3.5 To assure international trade partners of adequate data protection

A key element of data protection laws is the regulation of the transfer of personal data to other jurisdictions for processing or use. The rapid increase in the flows of financial resources and information across borders has resulted in regulatory spill-overs having consequences both for policy interdependence and for the role of the state.[1267] Legislation enacted in one country is capable of affecting trade and business with its partners.[1268] Nigeria's desire to be a financial and commercial hub in Africa can be jeopardized by the fact that it has no data protection regime. Countries with data protection laws may restrict the flow of personal data to the territory because of the absence of such legislation.

If Nigeria is to realise its am bition of becoming an international trading hub in Africa, it cannot avoid participating in the global exchange of personal data.

[1266] See Chp 1 p 1-2.

[1267] Farrell *Constructing the International Foundations of E-commerce: The EU-US Safe Harbor Arrangement* 277–306.

[1268] Regan 1993 (52) *Am J Econ Sociol* 258.

However, its capacity to do so will depend largely on its being able to satisfy its trading partners that it offers an adequate level of data protection. The fact that a growing number of its trading partner countries have already enacted data protection laws with provisions capable of prohibiting personal data exports to Nigeria if they are not satisfied with its level of protection, undoubtedly puts a lot of pressure on the country. As noted earlier, article XIV of the *General Agreement on Trade and Services* allows WTO member countries to adopt measures relating to the protection of personal data. It is interesting to note the reason given by the South African Law Reform Commission (SALRC) as its motivation in seeking the enactment of data protection laws that fits the EU standard. The Commission identifies international trade as a primary motivation. The SALRC noted that:

> Privacy is therefore an important trade issue, as information privacy concerns can create a barrier to international trade. Considering the international trends 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" information protection by international standards.[1269]

The Commission also noted that "[t]hose countries that refuse to adopt adequate data privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data."[1270] It therefore concluded that:

> a general comprehensive law making provision for adequate information protection should be instituted. This will be achieved by making provision for the inclusion of the information protection principles as well as for the means to ensure their effective application.[1271]

Even though the SALRC expressed the concern that adopting a data protection law, while satisfying the EU, would raise obstacles when trading with African countries, it

---

[1269] South African Law Reform Commission *Privacy and Data Protection* (Discussion Paper 109) vi.

[1270] Ibid at 9.

[1271] Id at 372.

nevertheless resolved to adopt a comprehensive data protection regime structured on the EU *Directive*'s principles. That resolve crystallised into the Protection of Personal Information Act 4 of 2013 in November 2013.[1272] South Africa, it should be noted, is Nigeria's foremost trade competitor in Africa. For a country seeking to become a preferred destination for outsourcing, an adequate data protection regime may be just what Nigeria needs to compete favourably with South Africa in the highly competitive global outsourcing industry.

Getting the privacy laws right is important both for individuals and for businesses. The challenge for businesses is to ensure that the benefits obtained through using new technology do not compromise individuals' expectations about the security and use of their personal information. Businesses must be able to assure their customers that their privacy will be respected.

4.4 The newly proposed data protection law for Nigeria

In February 2013, the government of Nigeria announced that it was in the process of enacting a law to "regulate the processing of personal information of individuals with regard to collection, holding, use or disclosure of such information by persons and private organisations."[1273] The proposed law is the Personal Information and Data Protection Bill which is sponsored by the National Identity Management Commission.[1274] According to the NIMC, the draft Bill will not only protect the individual's personal data but would also act as a framework for the implementation of the country's National Identity Card registration exercise. The full title of the Bill is: A Bill for an Act to Provide for Regulations Governing the Processing of Personal Information of Individuals, including the Collection, Holding, Use or Disclosure of Such Information by Persons and Organisations other than Government Institutions in a Manner that Recognises and Protects the Personal Information and Data of Individuals.

1272 Ibid at par 7.2.4(b). The new Act is available at the website of Polity.org.za [online].

1273 Ezigbo 24th February 2013 *Thisday*.

1274 Draft Bill available at NIMC website [online].

From the title of the Bill, it is immediately clear that the Bill, if enacted as it is, will exclude data held by governments at the federal, state and local government levels. Section 2(2) of the proposed law provides that:

> This Act does not apply to
>
> (a) any government institution;
>
> (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or
>
> (c) any organisation in respect of personal information that the organisation collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.

The proposed law assumes, without any verifiable basis, that data in the custody of government is safe and does not require the protection of the data protection law. The reality however, is that the three tiers of government, while being the biggest collectors, holders and users of personal information in Nigeria, are also the weakest link in the chain of protection for personal data. Leaving them out of the purview of the proposed data protection law diminishes the scope and depth of protection that the law promises.

Section 4(1) of the proposed law creates the office of a Privacy Commissioner to head the Privacy Protection Office. Under s 4(4)(1)(a), the Commissioner is expected to monitor and supervise compliance with the provisions of the proposed law while s. 14(1) provides that:

> the Commissioner shall, <u>within one year after the day on which a complaint is filed or is initiated by the Commissioner</u>, prepare a report that contains (a) the Commissioner's findings and recommendations;
>
> (c) any settlement that was reached by the parties; (underlining supplied)

The lack of capacity in the Privacy Commissioner to enforce the data protection law and the unnecessarily long period allowed for investigating a complaint casts a serious doubt on whether the proposed law can meet global benchmarks. It is doubtful that in its present form, the proposed law, if enacted, can meet the requirements for recognition as providing an adequate level of protection.

Another disturbing provision in the proposed law is s 4(4)(2)(d) which permits the Privacy Commissioner to "accept gifts and donations, whether subject to any trust or not". There is no exclusion of gifts from members of the industry that will come under the oversight purview of the Commissioner. The provision is so poorly crafted that one readily gets the impression that the Commissioner is at liberty to accept such gifts for his personal use without reference to any supervising authority. This is clearly an invitation to unscrupulous collectors and users of personal information to corrupt or compromise the system. The provision should be discarded or amended to place strict limits on who can give and what type of gifts can be given.

The efforts made so far to secure the enactment of a data protection law for Nigeria have largely been uncoordinated and lacking in a clear understanding of the socio-cultural milieu that defines the Nigerian society. At present there are 2 different Bills in respect of data protection before the National Assembly and a set of data protection guidelines released by the NITDA all seeking to protect personal data.[1275] Data protection is a novel idea in Nigeria and its essence and ramifications in the peculiar context of the Nigerian society must first be evaluated and understood by all the stakeholders in the ICT industry and the users of the various technologies in order for data protection to get a good footing in Nigeria. It is hoped that the recommendations made in chapter 8 will provide a way forward in achieving the goal of enacting a data protection law that will meet global standards and effectively protect all residents of Nigeria.

[1275] See the National Assembly website [online] and NITDA website [online].

CHAPTER 8

ENACTING A DATA PROTECTION LAW FOR NIGERIA

1. INTRODUCTION: MOTIVATIONS FOR ENACTING DATA PROTECTION LAWS

According to Colin Bennett,[1276] there are two primary motivations for legislating restrictions on the flow of data across national boundaries. The first is the concern for the privacy of the citizens, and second, securing the economic well-being of a nation. Data protection laws have primarily been enacted to ensure that the power inherent in holding information about people is not misused, particularly when such personal information is stored outside the territory of a given country.[1277] With regard to securing the economic well-being of the nation, there are usually two reasons driving the resort to legislation. The first reason is to secure the growth and protection of the ICT industry in the country.[1278] The second reason is so that the country proposing to enact the legislation can continue to have market access in those countries that have already enacted data protection laws capable of prohibiting trans-border data flows to it.[1279]

[1276] Bennett *Regulating Privacy* 55-58.

[1277] Mowlana *Global Information and World Communication: New Frontiers in International Relations* 115.

[1278] For example, the Nigerian IT Policy seeks, amongst other things, to: 1. empower Nigerians to participate in software and IT development, 2. encourage local production and manufacture of IT components in a competitive manner 3. establish and develop IT infrastructure and maximize its use nationwide. See NITDA *National IT Policy* iii-vii. See also Ajami 1990 (5) *IJTM* 589-590. The author argues that the free flow of data across national boundaries through the use of ICTs can bring benefits such as efficiency, accuracy and timelines in the transfer of data, assisting the smooth flow of commerce, and the generation of economic activity. On the other hand, there are disadvantages and costs such as the changes that arise in the value structure of the interacting societies and a weakening of ideas such as national autonomy and diversity.

[1279] Prior to April 2011, New Zealand's efforts to have the EU certify its data protection regime under the Privacy Act of 1993 as adequate met with negative responses from the Article 29 Working Party of the EU. In his 1998 review of the operation of the Act, the New Zealand Privacy Commissioner commented that "[i]n my view, the Privacy Act should be amended to address more precisely the circumstances in

The concern for the privacy of the citizens can usually be situated in the cultural ethos of the particular society. However, the levels of privacy protection across nations and cultures are not the same. The ways in which different societies create, safeguard, and enhance their respective states of privacy and the extent to which they are willing to protect their privacy vary from culture to culture.[1280] Nonetheless, there is a pan-human desire and need for privacy which is fundamentally rooted in social factors.[1281]

2. EXAMINING WHAT ROLE CULTURE AND ECONOMICS WILL PLAY IN SECURING THE ENACTMENT OF DATA PROTECTION LAW IN NIGERIA.

The perceptions and interpretations of the concept of privacy and data protection in Nigeria are determined by the cultural ethos of Nigerians. This in turn determines

---

which trans-border data flows should be prohibited or subjected to additional controls. In doing so it is unnecessary to adopt the restrictive EU model which has also been adopted in Hong Kong." See Stewart *International Transfers of Personal Data* [online]. Consequently, the Privacy (Cross-Border Information) Amendment Act of 2010 was enacted. It amended the Privacy Act of 1993 to make provision for an individual to make "information privacy requests" and introduced provisions to refer cross-border complaints to the relevant authority and to empower the Privacy Commissioner in exceptional cases to prohibit the onward transfer of personal information received from overseas. These were two key defects in the 1993 Act which prevented the Working Party from making a finding of adequacy. However, with the further legislation to amend the original law, the Article 29 Data Protection Working Party, in its Opinion 11/2011 on the level of protection of personal data in New Zealand, adopted on 4 April 2011, the Working party finally certified that New Zealand provides an adequate level of data protection. The decision paved the way to boosting New Zealand's trade with the EU. This market-access element of the EU's decision was made clear by the European Commission in its press release of 19th December 2012 in which it stated:

> There are also benefits for the economy and trade. Rules which recognise the adequacy of data protection standards make life easier for EU businesses by providing legal certainty in their international operations. By rubber-stamping the data protection rules of a third country, the EU is giving a substantial vote of confidence to its overall regulatory environment which facilitates personal data transfers and boosts the EU's trade with that country. (Underlining supplied).

See European Commission Press Release *EU approves New Zealand's data protection standards in step to boost trade* [online].

[1280] See for example, Moore *Privacy: Studies in Social and Cultural History* 276. See also Flaherty D *Privacy in Colonial New England* (1972); Westin A *Privacy and Freedom* (1967) and Altman 1977 (33) *J Soc Issues* (1977) 66-84.

[1281] See Moore Privacy: *Studies in Social and Cultural History* 276. Moore sees the need for privacy as socially created and suggests that an extensive, highly developed concern for privacy is only possible in a relatively complex society with a strongly felt division between a domestic private realm and public sphere - "privacy is minimal where technology and social organization are minimal."

the degree of importance that Nigeria attaches to the protection of information privacy. In a study it commissioned to assess the methods it uses to test the adequacy of data protection in other countries, the EU acknowledged the fact that different political and cultural values would impact on interpretations of privacy and the standards of "adequacy" of data privacy protection in different countries:

> A final difficulty is that of cultural and institutional non-equivalence. Judgments about adequate protection must remain sensitive to important cultural differences. Despite the growing convergence of international data protection policy, 'privacy' still means something very different in various cultural and national traditions, perhaps particularly in non-Western jurisdictions but by no means there alone.[1282]

In 1995, Milberg, Burke, Smith and Kallman,[1283] examined the effect a country's regulatory environment has on an individual's information privacy concerns. In a subsequent research,[1284] they developed a conceptual model and test with a cross-cultural sample from 19 different countries. They found that a country's regulatory approach to the corporate management of information privacy is affected by its cultural values and by individuals' information privacy concerns. Since then, other studies have focused on the effect of an individual's nationality/cultural values on his/her information privacy concerns when purchasing goods and services over the Internet.[1285]

Many authors have identified a relationship between national culture and attitude to information privacy. Geert Hofstede[1286] identified five dimensions of human

---

[1282] Raab et al *Adequacy of the Level of Protection of Individuals* 202 [online].

[1283] Milberg, Burke, Smith and Kallman 1995 (38) *Commun ACM* 65-74.

[1284] Milberg, Smith and Burke 2000 (11) *Organization Science* 35-57.

[1285] See Bellman, Johnson, Kobrin and Lohse 2004 (20) *Information Society* 313-324. They used the conceptual model established by Milberg *et al* (n 1308 above) to measure the information privacy concerns of individuals from 38 countries. The aim of their study was to test a number of hypotheses formulated by the Milberg team which related to how a country's national regulation affects the information privacy concerns of its citizens. The study confirmed that a country's regulatory approach to the corporate management of information privacy is affected by its cultural values and by individuals' information privacy concerns.

[1286] See Hofstede *Culture's Consequences: International Differences in Work-Related Values*. He defines culture as "the interactive aggregate of common characteristics that influences a human group's response to its environment. Culture determines the identity of a human group in the same way as personality

behaviour that characterise a culture; they are *Power Distance*, *Uncertainty Avoidance*, *Individualism/Collectivism*, *Masculinity/Femininity* and *Long-term or Short-term Orientation*.[1287] Walczuch, Singh and Palmer,[1288] using Hofstede's five dimensions of human behaviour in culture, have argued that most countries that have adopted data protection legislation so far have low *Power Distance*[1289] measures that are below the threshold value in Hofstede's[1290] studies. This suggests that cultures that do not accept an unequal distribution of power (i.e., the culture agrees that everyone should have the same rights and privileges), are more inclined to enact data protection legislation.[1291]

For the developing countries, their high *Power Distance* and low *Individualism*[1292] levels suggest that such countries have a low inclination towards data protection legislation. Indeed, African countries taken as a whole have the least developed legal regimes for data privacy protection. Even the *African Charter on Human and People's Rights* of 1981 fails to make provision for a right to privacy in its catalogue of fundamental human rights.

---

determines the identity of an individual." (25-26). See other authors on the relationship between culture and privacy: Roberts and Gregor *Privacy: A Cultural View* 199-225; Altman 1977 (33) *J Soc Issues* (1977) 66-84.

1287 Hofstede *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations* 79.

1288 Walczuch, Singh and Palmer 1995 (8) *Inform Tech & People* 37-57.

1289 *Power distance* explains how a culture approaches and accepts inequality in status (i.e., prestige, wealth and power).

1290 Hofstede *Cultures and Organizations: Software of the Mind*; Hofstede *Culture's Consequences: International Differences in Work Related Values*.

1291 Hofstede *Culture's Consequences: International Differences in Work Related Values* 65.

1292 Id at 148. *Individualism*, in contrast to *collectivism*, is identified as "the relationship between the individual and the collectivity that prevails in a given society and is reflected in the way people live together as for example, in nuclear families, extended families, or tribes".

2.1 The role of culture in the enactment of data protection legislation in Nigeria

In a review of the writings of some African scholars on African culture and personality traits and the patterns and processes of African cultural adaptation in the face of globalisation, James Lassiter[1293] shows that the predominant view appears to support the views of Walczuch *et al*. The aim of these writers is to identify and explain African psychological processes, personality characteristics, and the processes of African cultural adaptation to indigenous social conditions and external influences. Scholars such as John Mbiti[1294] and Joseph Nyasani,[1295] argue that African concepts of the individual and self are almost totally dependent on and subordinate to social entities and cultural processes. According to Mbiti, the individual has little latitude for self-determination outside the context of the traditional African family and community. In his words:

> Whatever happens to the individual happens to the whole group, and whatever happens to the whole group happens to the individual. The individual can only say: 'I am, because we are; and since we are, therefore I am.' This is a cardinal point in the understanding of the African view of man.[1296]

On his part, Nyasani argues that the African individual hardly knows how to act outside the context of his community's prescriptions and proscriptions. This is because he is caught in a social pyramid characterised by a one-way vertical structure of authority and a two-way horizontal family and communal support system. The existence of the individual in African society, Nyasani declares, is a "quasi-dissolution into the reality of others for the sake of the individual's existence."[1297] Furthermore,

---

[1293] Lassiter 2000 (3) *ASQ*.

[1294] Mbiti *African Religions and Philosophy*.

[1295] Nyasani *The African Psyche*.

[1296] See n 1294 at 106.

[1297] See n 1295 at 60. For a slightly different perspective on the subject, see Gyekye *The Unexamined Life: Philosophy and the African Experience* 32. While agreeing that the African individual is inextricably bound to his family and community, Gyekye argues that it would be more correct to describe the social order in an African community as amphibious because it manifests features of both communality and

Nyasani maintains that the vertical power structure of the typical family in an African society exerts such enormous influence on the African child that it muzzles him/her from the outset and engenders a docile attitude towards the power structure of the family, community and ultimately the state.[1298] The image created by these two writers is that of an African individual so subsumed in the communal whole that he appears to have no choice but accept the prevailing power structure in the community.

Analysing the countries that had enacted data protection laws as at the time of their writing, Walczuch, Singh and Palmer, using Hofstede's five dimensions of human behaviour in a culture, hypothesized that all adopters of data protection legislation have a high individualism measure. This suggests that countries that put a higher value on individuals' interest are more likely to enact data protection legislation. This makes sense, they argue, since the main purpose of data protection legislation is to protect the individual's rights. On the other hand, they posited that developing countries have high *Power Distance* and low *Individualism* measures.[1299] The low *Individualism* measure for developing countries such as the countries of sub-Saharan Africa is consistent with the generally acclaimed communal structure of African societies, including Nigeria.

With a population of about 167 million people, 250 ethnic groups and about 500 languages,[1300] there is nothing like a pan-Nigerian culture. There is therefore no pan-Nigerian culture of privacy that can serve as the spring-board for motivating data protection legislation for Nigeria.[1301] Furthermore, the dearth of judicial activism in support of privacy and the lack of robust privacy advocacy from individuals and civil society groups, make Walczuch *et al's* proposition about high power distance and

---

individuality (32).

1298 See n 1295 at 129.

1299 The authors caution that their findings merely identify patterns that provide a conceptual framework for further empirical analysis of the hypothesized relationships.

1300 See the Nigerian Population Commission website [online]. See also the Central Intelligence Agency (CIA) *The World Factbook* [online].

1301 It is not suggested here that Nigerian cultures do not have or observe cultural practices that protect privacy generally. Such practices, where they are available, are as varied as the different ethnic groups that make up Nigeria.

developing countries plausible for Nigeria.[1302] It is doubtful that cultural motivation without more would advance the cause of data protection legislation in Nigeria. Culture will therefore play a limited role in the adoption of data protection legislation in Nigeria.

2.2 The role of economic and commercial considerations in the adoption of data protection legislation in Nigeria

The Nigerian economy began the process of re-integration into the global economy with the re-emergence of democratic governance in 1999 and the accompanying market-led reforms from 2003. The re-integration has a clear economic development objective which is encapsulated in a set of national aspirations that seek to make Nigeria one of the top twenty economies in the world by the year 2020. These aspirations are articulated in the Vision 20:2020 document.[1303] One of the key strategies that will drive the actualisation of these aspirations is the pursuit of a market-friendly and globally competitive business environment. As has been argued earlier, data protection and privacy issues are no longer just national issues; they have become globalised by the rapid diffusion of technology. Also, it is now beyond dispute that data protection legislation enacted in one country is capable of affecting trade and business with its partners.

The policy documents of the Nigerian government pertaining to information technology, trade and outsourcing clearly attest to the realisation that the country's economic development and well-being will be better served by adopting systems and benchmarks that are compatible with global standards. In order to ensure that the Nigerian economy and its commercial interests are not unduly disadvantaged in the international market, Nigeria must take steps to meet global standards on data protection. It is this economic reality that will motivate the pursuit of a data protection law for Nigeria.[1304]

[1302] This proposition calls for further research to establish the extent of its applicability to Nigeria, if any at all. Such a study falls outside the ambit of this thesis.

[1303] See Nigeria Vision 20:2020 [online].

[1304] See NITDA *National Policy for Information Technology* (2001) chap 13 at 32.

Recognizing the need to meet global standards, the Nigerian government must take the next step by enacting a data protection law that will have as its underlying principles the OECD *Guidelines on the Protection of Privacy and Transborder Flows* released in 1980.[1305] The OECD Guidelines were formulated as part of the efforts in the 1980s to create a uniform and comprehensive data protection regime in Europe but because the Guidelines were non-binding, it did not produce the desired effect. The application of diverse data privacy laws in the different countries threatened the flow of data in Europe and prompted the enactment of *Directive 95/46/EC* which is based on the OECD *Guidelines*. The principles enunciated in the Guidelines form the bedrock of the *Directive*. Although Nigeria is not a member of the OECD, the Guidelines[1306] present a quick and easy summary of the minimum

---

13.1 policy statement

The nation shall promote and guarantee freedom and rights to information and its use, protect individual privacy and secure justice for all by passing relevant bills and acts

13.1 objectives

(viii) To enhance freedom and access to digital information at all levels while protecting personal privacy

13.3 strategies

(i) Sponsor and promote the establishment of the following IT Bills and Acts to realize objectives such as freedom of access and rights to information, on-line transaction, service, payment system, privacy and confidentiality, digital signatories, and intellectual property rights

(ii) Ensure the protection of individual and collective privacy, security, and confidentiality of information.

[1305] See n 1220. The principles enunciated in the Guidelines are reflected in the EU *Directive on Data Protection*.

[1306] The *Guidelines* consist of 8 broad principles:

(1) Collection Limitation Principle - 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.

(2) Data Quality Principle - Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

(3) Purpose Specification Principle - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as specified on each occasion of change of purpose.

(4) Use Limitation Principle - Personal data should not be disclosed, made available or otherwise used except, with the consent of the data subject; or by the authority of law.

(5) Security Safeguards Principle - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

(6) Openness Principle - There should be a general policy of openness about developments, practices and policies with respect to personal data. 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.

standard that is expected in a domestic data protection law and thus provide a starting point for data protection legislation for the country. The concept of data protection and its relationship with privacy is relatively new to most individuals and organizations in Nigeria. Any new legislation in this area will significantly alter many business management practices in the country and impact individual perceptions and responses to personal data.

2.3 Objectives of a data protection regulatory framework

The objectives of a data protection regulatory framework should primarily be to: -

1. Provide adequate security and privacy in handling personal information;
2. Create confidence among consumers and users of both networked and non-networked industries;
3. Accelerate uptake of electronic transactions; and
4. Promote a secure electronic environment in line with national IT objectives.[1307]

Furthermore, the regulatory framework, in order to align with internationally accepted benchmarks, must have the following characteristics:

1. The ability of the system to deliver a good level of compliance with the rules.
2. The regulatory system must be able to give sufficient support and help to individual data subjects in the exercise of their rights.

---

(7) Individual Participation Principle - 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 within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (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.

(8) Accountability Principle - A data controller should be accountable for complying with measures which give effect to the principles stated above.

[1307] These core objectives were identified by the Malaysian government when it was in the process of drafting legislation on Personal Data Protection to regulate the collection, possession, processing and use of personal data. See UN Economic and Social Commission for Asia and the Pacific *Good Practices in Information and Communication Technology Policies in Asia and the Pacific* (ST/ESCAP/2347) 56.

3. The system must be able to provide appropriate redress for the injured party where the rules are not complied with.[1308]

3. FOREIGN DATA PROTECTION LAWS AS MODELS FOR NIGERIA

The legal and regulatory systems of the countries of the world are different. These differences are often rooted in perceptions based on customs, culture, religion and politics.[1309] No single country has a pure legal tradition or history that is not influenced by other systems external to it. The Nigerian legal system is a mixture of the statute and common law derived from the UK, customary law (indigenous) and Islamic sharia law (derived ultimately from Arabia, the source of Islam). However, it is possible for two countries to have different legal systems and yet have similar elements in their legal frameworks. For example, two countries may have a different government structure such as a federal republic, like Nigeria as opposed to the UK with a unitary state model; yet both countries operate the common law model in their legal systems.

Nigeria's legal and judicial systems have not kept pace with the rapid development and deployment of the various technologies that make the Internet and other ICT-powered activities possible. It must therefore look to those countries that are well exposed to ICTs, the Internet and the digital marketplace and have developed legal responses to the issues affecting interaction in the digital marketplace. Doing so will enable it to draw inspiration and direction on how to address the issues arising from the use of technologies in the global network economy.

3.1 Regulatory convergence

Across the world, regulatory policies have become increasingly interdependent because many of the regulatory problems, either the problems that a given regulatory regime is aiming to address or the problems caused by regulation, are of a cross-

[1308] See European Commission Data Protection Working Party *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* DG XV D/5025/98 WP 12 (1998).

[1309] David "Structure and Divisions of the Law" 2-2.

border nature. George Bermann[1310] makes the case, for example, that if a government wants to improve air quality or stabilize the financial system, it has to find a way to get foreign governments to accept its regulatory ideas. Increasingly therefore, regulatory cooperation is a preferred mode of dealing with cross-border issues particularly as they affect the global flows of information.

It is now common to find that policy makers in one country imitate or adapt the efforts of other countries. Data protection is an example of policy imitation. As Colin Bennett[1311] has demonstrated, the incentives to copy or at least draw lessons from the pioneers in such circumstances can be strong. Bennett argues that when innovation is required, there may be no readily available solution within the existing repertoire of policy and procedural techniques. Without the opportunity to learn from one's own experience, there is a natural tendency to look abroad, to see how other states have responded, to share ideas and to bring foreign evidence to bear on the domestic decision-making process. This is what regulatory convergence is all about. It is, he argues, the result of a pressure to conform in an insecure and tentative policy-making climate.[1312]

The various states that have enacted or are planning to enact data protection laws, have converged around a common set of "fair information principles" which form the basis of all data protection law.[1313] Bennett categorised the data protection systems of different countries into five models:

1. The Voluntary Control Model
2. The Subject Control Model
3. The Licensing Model
4. The Registration Model
5. The Data Commissioner Model[1314]

[1310] Bermann 1996 (9) *Admin L J Am U* 957.

[1311] See Bennett *Regulating Privacy* 123-143.

[1312] Ibid at 5. See also Bygrave (2000) *PLPR* 129.

[1313] See n 1311 at 6.

[1314] See n 1311 at 153.

In his analysis of the various data protection models, he described the necessary factors or characteristics of each model and aligns countries with one model or another.[1315] In developing a data protection framework for Nigeria, it is important to learn from the experiences of other countries. While adverting to the legal developments in other countries as a guide to how Nigeria should proceed, it is necessary to acknowledge that although the challenges of protecting personal data is almost universal, countries have developed different legal responses at different rates. A brief review of some of these responses follows.[1316]

3.2 Information/Data Protection in Other Countries: A Brief Overview

3.2.1 Information privacy protection in the US[1317]

The US legal framework for the protection of privacy is complex. Although the US does not have an overarching privacy law like the EU and Canada, compliance with the patchwork of sectorial laws and regulations, state laws and state and federal constitutional provisions is challenging.[1318] Much of the privacy regulation in the US occurs at the state level, where many of the 50 states have enacted privacy laws that govern specific industries, issues or practices. Often, these laws are inconsistent, so that a set of business practices that is legal and commonplace in one state may be prohibited just across the state line. In 2004 alone, more than 20 states passed separate financial privacy laws.[1319]

In the bid to protect privacy, the US Congress has enacted federal privacy legislations specific to certain industries. For example:

- The *Gramm-Leach-Bliley Act* of 1999 applies to financial institutions;

[1315] See n 1311 at 153-192.

[1316] See chp 1 par 4 above.

[1317] See Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (Thesis) 27-144, for an in-depth study of privacy protection in the US.

[1318] Westby *International Guide to Privacy* xx.

[1319] Smith *Protecting Consumers and the Marketplace* [online].

- *Health Insurance Portability and Accountability Act* of 1996 (HIPAA) applies to health care providers;[1320]
- The privacy provisions of the *Cable Act* of 1992 apply to cable operators; [1321]
- The privacy provisions of the Communications Act of 1996[1322] apply to telecommunications carriers.

However, this *ad hoc* approach to privacy legislation has many drawbacks. It has led to an overlapping, inconsistent and incomplete patchwork of state and federal laws that creates compliance difficulties for businesses and uncertainty for consumers. Consumers and businesses alike are often faced with the daunting task of determining whether one or more of the existing laws applies.[1323]

The answer may depend on the type of data involved, the kind of company that collects it, where and how it is collected, and how it might be used. For example, personal information collected by a bank is covered by one privacy standard, but that same information collected by a hospital is covered by a different standard.[1324] If that information is from a child under the age of 13, it is protected by yet another standard if it is collected online, but it may not be protected at all if it is collected offline.[1325] In spite of all these legal distinctions, the consequences of misuse of that information could be exactly the same in each scenario. Two of the most important and broad-based of these laws are the Privacy Act of 1974[1326] and the Computer Matching and Privacy Act.[1327] These laws deal exclusively with personal information

---

1320 *Health Insurance Portability and Accountability Act* of 1996. The Act covers health care providers, insurers and information clearinghouses. These entities were expected to be in full compliance of the Act by April 2003. The *Rules for Patient Privacy* under the legislation were published in 2001.

1321 Also known as Cable Television Consumer Protection and Competition Act of 1992.

1322 The Communications Act of 1934 was amended by the Telecommunications Act of 1996.

1323 See generally Kobrin 2004 (30) *Rev Int'l Stud* 111. See also Reidenberg 2000 (52) *Stan L Rev* 1315-1371; Schwartz and Reidenberg *Data Privacy Law: A Study of United States Data Protection* (1996).

1324 See n 1319 at 2.

1325 Ibid.

1326 The Privacy Act regulates the "collection, maintenance, use, and dissemination of information" about individuals by federal agencies. See *Doe v Chao* 540 US (2004) 614 at 618 (quoting s 2(a)(5) of the Privacy Act of 1974. It "authorizes civil suits by individuals . . . whose Privacy Act rights are infringed". Also see *Sussman v US Marshals Serv* 494 F 3d (DC Cir 2007) 1106 at 1123.

1327 The *Computer Matching and Privacy Protection Act* of 1988 amended the Privacy Act of 1974 by

held by the federal government and do not have any authority over the collection and use of personal information held by other private and public sector entities.

The Privacy Act was enacted to address the problems posed by electronic technologies and personal records systems; it covers the vast majority of personal records systems maintained by the federal government. The Act set down some basic principles of "fair information practice" and provides individuals with the right of access to information about themselves and the right to challenge the contents of records. It requires that personal information may only be disclosed with the individual's consent or for purposes announced in advance. The act also requires federal agencies to publish an annual list of systems maintained by the agency that contain personal information.

The Computer Security Act of 1987[1328] also deals with personal information in federal record systems. It protects the security of sensitive personal information in federal computer systems. The Act establishes government-wide standards for computer security and assigns responsibility for those standards to the National Institute of Standards. The law also requires federal agencies to identify systems containing sensitive personal information and to develop security plans for those systems.

3.2.1.1 Enforcement of information privacy protection in US

The US has no single independent agency to oversee information privacy issues. Two major federal agencies responsible for enforcement of information privacy protections in some of the legislations are the Office of Management and Budget (OMB) and the Federal Trade Commission (FTC). The OMB plays a limited role in

---

prescribing the manner in which computer matching involving Federal agencies could be performed and by adding certain protections for individuals applying for and receiving Federal benefits. According to Privacilla.org, the Act is notable for the fact that it institutionalises the sharing of data among US federal government agencies. Information collected for one purpose may be used for different purposes by a different federal agency. As noted by Privacilla, although the integrity and fairness of stored information seem to be assured by the Act, privacy is not. See Privacilla *Privacy and Government* [online].

1328 In 1987, the US Congress enacted the Computer Security Act to reaffirm that the National Institute for Standards and Technology (NIST), a division of the Department of Commerce, was responsible for the security of unclassified, non-military government computer systems. Under the law, the role of the National Security Agency (NSA) was limited to providing technical assistance in the civilian security realm. Congress rightly felt that it was inappropriate for a military intelligence agency to have control over the dissemination of unclassified information. See EPIC *Computer Security Act* [online].

setting policy for federal agencies under the Privacy Act. However, information privacy is a central element of the consumer protection mission of the Federal Trade Commission (FTC).[1329]

The Commission educates consumers and businesses about the importance of personal information privacy, including the security of personal information. Under the *FTC Act*, the Commission enforces companies' privacy promises about how they collect, use and secure consumers' personal information. The Commission enforces the *Gramm-Leach-Blilely Act* by implementing rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information. The Commission also protects consumer privacy under the Fair Credit Reporting Act[1330] and the Children's Online Privacy Protection Act of 1998.[1331]

3.3 Data protection in the UK

3.3.1 Data Protection Act 1998

The Data Protection Act, 1998 (DPA)[1332] replaces the earlier Act of 1984. It implemented the 1995 European *Directive on Data Protection* which is designed to regulate the collection, storage, processing and distribution of personal data.[1333] The Act places obligations on those who record and use personal data, and it gives rights to individuals about whom information might be held. The DPA[1334] creates the office of Information Commissioner who is a government official. Amongst other things, the Information Commissioner maintains a register of data controllers and the data that they hold. The Act prescribes eight Data Protection Principles, which set out

1329 See FTC website [online].

1330 The Fair Credit Reporting Act (as amended December 18, 2010).

1331 Children's Online Privacy Protection Act 15 USC § 6501–650..

1332 Available at the OPSI website [online].

1333 S (1)(1) of the Act defines data as any structured information, not necessarily electronic, that is intended to be processed or held in a filing system. It must not only be structured, but must also be sorted or indexed to enable processing and/or retrieval. Personal data is defined as any data, relating to a living individual, which can, directly or indirectly, identify that individual. A Data Controller is a person who (either alone or jointly) determines the purposes for which personal data are processed, and the manner in which they are processed.

1334 For an excellent review of data protection in the UK, see Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 251-266.

what is expected of all data controllers and their employees.[1335]

3.3.1.1 Regulatory and enforcement institutions

The Information Commissioner's Office (ICO) is the independent regulatory authority set up under the Data Protection Act to uphold information rights in the public interest. One of the key functions of the office is to promote openness by public bodies and data privacy for individuals. Under the Act, data controllers are required to notify the Information Commissioner of their use of any personal data, unless that use is granted an exemption. This means that they must tell the Commissioner what data is being stored and the purpose for which it is being stored. The ICO is concerned with, amongst other things, the enforcement of the following legislations and subsidiary legislations:

- Data Protection Act, 1998.
- Privacy and Electronic Communications Regulations, 2003[1336]
- Freedom of Information Act, 2000.[1337]

[1335] Part I of Schedule 1 of the Act sets out the eight data protection principles:

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

[1336] The Privacy and Electronic Communications Regulations, 2003 regulate direct marketing activities by electronic means (by telephone, fax, email or other electronic methods). They also regulate the security and confidentiality of such communications, with rules governing the use of cookies and spyware. The *Regulations* complement the Data Protection Act, 1998 (DPA) in the regulation of the e-marketing activities of organisations' that use personal data and in ensuring appropriate safeguards for individuals' rights and privacy. They do not over-ride the DPA. The regulations legislate against unsolicited emails or Standard Messaging Service (SMS) i.e. text messages, commonly referred to as spam. They also prohibit sending direct marketing communications by email where the identity of the person who sent it is disguised or concealed. Marketing emails that do not provide the recipient with a valid address by which they can request such communications to cease are also prohibited.

- Environmental Information Regulation, 2004.[1338]

The ICO is empowered to promote compliance with the above laws by seeking to change the behaviour of organisations and individuals that collect, use and keep personal information. The powers of the ICO to enforce compliance with the data protection laws include criminal prosecution, civil monetary penalties, non-criminal enforcement and, in some circumstances, audit.[1339]

3.4 Data protection in Australia

Although privacy is protected in Australia, the Australian Federal Constitution and the constitutions of the six Australian States do not contain any express provisions relating to privacy. In 1988 however, a principal federal statute, the Privacy Act 1988 was enacted.[1340] The Act gave effect to Australia's agreement to implement the guidelines adopted in 1980 by the Organization for Economic Cooperation and Development (OECD);[1341] it was also aimed at implementing Australia's obligations under Article 17 of the *International Covenant on Civil and Political Rights*.

The Australian Privacy Act defined a set of eleven Information Privacy Principles (IPPs), based on the OECD *Guidelines*, which principles apply only to the activities of the agencies of the federal government of Australia.[1342] There is no omnibus instrument that safeguards privacy rights, such as a Bill of Rights. The absence of a constitutional right to privacy has weakened data protection in the country by engendering a highly restrictive mode of judicial review.[1343] Graham Greenleaf argues that the absence of a Bill of Rights has ensured that Australian courts do not have a "convenient platform in domestic law from which to develop privacy law as an

---

1337 Freedom of Information Act, 2000 (UK).

1338 Environmental Information Regulations, 2004 (UK).

1339 See ICO *Data Protection Regulatory Action Policy* 1 [online].

1340 Commonwealth of Australia, Privacy Act 1988.

1341 See n 1220.

1342 A separate set of rules concerning the handling of consumer credit information, was added to the law in 1999 and applies to all private and public sector organizations. The third area of coverage is the use of the government issued Tax File Number (TFN), where the entire community is subject to Guidelines issued by the Privacy Commissioner, which take effect as subordinate legislation.

1343 Webb 2003 (2) *JILT* 5.

aspect of human rights".[1344] Privacy was protected by the courts merely as a "by-product" of the protection of other interests such as breach of confidence, defamation, nuisance and trespass which is far from a general law of data protection.[1345]

In the year 2000, the Privacy Amendment (Private Sector) Act (Commonwealth),[1346] was enacted and it extended the regulation of personal data to the private sector. One major objective of the new law was to apply a set of National Privacy Principles (NPP) developed by the Privacy Commissioner in 1997 and 1998, originally as a self-regulatory substitute for legislation.[1347] With the extension of the Privacy Act 1988 to the private sector, all organisations not covered by an exemption in the law are required to comply with the National Privacy Principles in regard to how they handle personal information.

Even though it sought to meet the requirements of adequate levels of data protection as stipulated by the EU *Directive 95/46/EC*, the National Privacy Principles impose a lower standard of protection than the EU *Directive*. Controls on the transfer of personal information overseas are limited, requiring only that organizations take "reasonable steps" to ensure personal information will be protected, or that they "reasonably believe" that the information will be subject to similar protection as applied in the Australian law.[1348]

1344 Greenleaf 2001 (4) *UNSWLJ* 1.

1345 Taylor 2000 (26) *Monash U L Rev* 247.

1346 Privacy Amendment (Private Sector) Act 2000.

1347 Dixon argues that the new legislation was driven by the strong business orientation of the Federal Government of Australia. He is of the view that three main influences account for the passage of the new law: first, the government of the state of Victorian was threatening to go ahead with its own private sector legislation; second, the EU Directive imposed complex legal requirements on trade in personal information with countries without "adequate" protections; third, there was pressure from information industry groups because research indicated privacy protection was vital to consumer confidence in new technologies. Through this combination of economic and political forces, Australia had a data protection framework in operation by December 2001 when the Act came into force. See Dixon *Australia's New Privacy Legislation* 5 [online].

1348 In its opinion on the adequacy of the Privacy Amendment (Private Sector) Act *2000* (Cth), the Article 29 Working Party of the EU welcomed the adoption of the Act, but noted a number of areas of concern in relation to the Act. The Working Party advised that data transfers to Australia could only be regarded as adequate if appropriate safeguards were introduced to meet the data privacy concerns highlighted in respect of small business and employee data. See Article 29 Working Party's *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000 (Opinion 3/2001)* 3.

3.4.1 Regulatory and enforcement institutions

The Office of the Privacy Commissioner (OPC) was established under the Privacy Act, 1988. It is an independent body whose function is to promote and protect information privacy in Australia. The Office of the Privacy Commissioner is the regulator with specific statutory mandate for the protection of the personal information of individuals in the custody of Australian government agencies at the federal level, and personal information held by all large private sector organisations, health service providers and some small businesses.

The Office handles all complaints and investigates all matters relating to personal information under its purview. The Privacy Commissioner's determinations are enforceable by the federal high courts and magistrate courts. The OPC also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations. Access to personal information held by state governments is through state privacy laws.[1349]

In its report on the reform of Australian information privacy law,[1350] the Australian Law Reform Commission (ALRC) recommended that the Privacy Act 1988 be "... redrafted and restructured to achieve significantly greater consistency, clarity and simplicity."[1351] The Commission recommended that the Information Privacy Principles and the National Privacy Principles be rationalized and merged into Unified Privacy Principles which will cover the handling of personal information in the public and private sectors. Furthermore, the Commission recommended the adoption of a principles-based regulatory method for the regulation of information privacy in Australia. It also looks to rely on both the tools of regulation, that is, the principles, and a more outcomes-based approach to privacy regulation.[1352]

[1349] See for example, the Privacy and Personal Information Protection Act, 1998 of New South Wales which deals with the way public sector agencies in NSW manage personal information.

[1350] ALRC *For Your Information* (Executive summary)[online].

[1351] ALRC *For Your Information* (Regulatory theory) [online].

[1352] Ibid.

3.5 Data Protection in South Africa

South Africa is the latest African country to enact a data protection law. The Protection of Personal Information Act (POPI) 4 of 2013 became law on 26 November 2013. The Act regulates how personal information is collected, processed, stored and secured. The POPI Act provides for a mandatory notification of data breach to data subjects.[1353] The Act also prohibits the processing of children's personal information[1354] and sets limitations on the processing of information regarding the health, sexual life or criminal behaviour of data subjects.[1355] Section 72 of the Act makes provisions for the transfers of personal information outside South Africa.

The Act establishes the Information Protection Regulator (IPR) with powers to investigate data protection breaches and enforce the provisions of the Act, including the power to impose fines. Section 114 of the Act provides that the law will take effect one year after the official commencement date. The South African data protection law is clearly designed to comply with the standards set by the EU *Directive 95/46/EC* although it remains to be seen whether it will passes the test when it is eventually evaluated by the European Commission's Article 29 Data Protection Working Party. Nevertheless, Nigerian businesses with subsidiaries or interests in South Africa should begin now to study how the Act will affect them, particularly the provisions concerning trans-border transfer of personal data out of South Africa.

[1353] See s 22 Protection of Personal Information Act 4 of 2013.

[1354] S 34.

[1355] Ss 32-33.

4. CHOOSING A DATA PROTECTION MODEL FOR NIGERIA

There is, as noted by Kuner,[1356] an increasing momentum for the adoption of data protection laws by states, notwithstanding the substantial cultural and legal differences between the various states and regions of the world. At the centre of this momentum is the European Union *Directive* on data protection. Kuner identifies three broad sets of public agencies that play a role in the enforcement and oversight of data protection legislation: supervisory authorities (data protection and privacy commissioners), central coordinating agencies, and tribunals or courts.[1357]

When Colin Bennett[1358] first distinguished between several models adopted by different supervisory authorities for data protection implementation in 1992, he alluded to the overlap in responsibilities in the different models adopted in the different countries. Writing in 2003,[1359] Bennett noted that data protection agencies have become more difficult to classify according to any one model. This is very much the outcome of the rising tide of policy and regulatory convergence described earlier.[1360] The various data protection authorities now perform an intricate blend of functions derived from a mixture of the different models.

Robert Baldwin and Martin Cave[1361] identified eight regulatory models that are the "basic capacities or resources that governments possess and which can be used to influence industrial, economic or social activity".[1362] However, in the last two decades, there has been a wide-ranging and long-running debate about how to regulate the collection, storage and use of personal data. Two main camps dominate the debate; the first calls for government regulation while the second espouses self-

---

1356 Kuner 2009 (25) *C L S Rev* 307-317.

1357 Ibid.

1358 Bennett *Regulating Privacy* 153-192.

1359 Bennett and Raab *The Governance of Privacy: Policy Instruments in Global Perspective* 164.

1360 See par 3.1 above.

1361 Baldwin and Cave *Understanding Regulation: Theory, Strategy and Practice*. The regulatory strategies are: i. Command and control, ii. Self-regulation iii. Incentives, iv. Market-harnessing controls, v. Disclosure, vi. Direct action, vii. Rights and liabilities laws, and viii. Public compensation.

1362 Ibid at 34.

regulation.[1363] There is also a third option, namely co-regulation.

4.1 Government regulation (the command and control model)

The first camp seeks legislation that would prescribe detailed and strict limits on the ways that companies can collect data online, the types and amounts of personal information they can collect, and how the collected data should be used. Those in favour of this approach maintain that strong government regulation is necessary to protect unsuspecting Internet users against the profit-oriented behaviour of companies that collect and trade in personal data.[1364]

Proponents of government regulation argue that the desire for profits, coupled with the economic value of personal information, will prevent private firms from taking adequate steps to protect personal data. They therefore seek the government's active intervention by way of legislation that would take a strong stand in protecting personal information.

Under this model, comprehensive laws are enacted in which the government establishes binding rules that regulated firms must obey and then uses the power of the state to enforce those rules. This approach typically specifies standards which regulated firms must comply with (the 'command'); failure or refusal to comply with the regulation will attract a penalty (the 'control'). It is characterized by an oversight body, which ensures compliance with the legislation by imposing sanctions on errant firms.

According to Neil Gunningham,[1365] the command and control model of regulation achieved some considerable successes in the past, especially in the area of regulating the environment, in terms of reducing air and water pollution. However, it has been widely criticised for inhibiting innovation, for its high costs, inflexibility, and diminishing returns. Andrew Murray argues that the reason why traditional "command and control" regulatory interventions fail is that lawmakers frequently

[1363] See for example, Solove and Rotenberg *Information Privacy Law* 2.

[1364] See Hirsch *Law and Policy of Online Privacy* [online].

[1365] Gunningham "Beyond Compliance: Next Generation Environmental Regulation" 49.

consider the environment to be regulated as a static and inert object. When therefore the environment reacts in ways not consistent with expected results, lawmakers tend to enact further interventions to re-model the environment. Yet, no sooner than the new regulatory intervention is introduced, than it too faces unpredictable reactions from the regulated industry and so on, until possibly, a solution is found.[1366]

The consequence is that the regulatory environment is disrupted and legal uncertainty prevails. This is why, according to Murray, command and control legal regulatory controls cannot be effective in cyberspace. The solution he proffers is that regulators should develop a regulatory 'hybrid' system in which legal controls form part of the regulatory web or matrix. According to him, regulators should be mindful of the "need for a more cohesive, measured, prudent and non-interventionist approach"[1367] to cyberspace regulation. The observed defects in the command and control model notwithstanding, the trend in a significant number of the countries that have enacted data protection laws is toward some form of omnibus or comprehensive data protection regime.[1368]

4.2 Self-regulation

The second camp in the debate about the regulation of information privacy argues that self-regulation will yield better results than government rules. Robert Litan, for example, posits that:

> in the fast-moving Internet environment, policy-makers' first instinct should be to rely on markets and technology to address troublesome issues and to act only if there are identifiable market failures that can be corrected usefully by some type of government intervention.[1369]

The proponents of self-regulation assert that the rapid and continuous technological innovations in ICTs and the Internet make the Internet economy ill-suited to

---

[1366] Murray *The Regulation of Cyberspace: Control in the Online Environment* 229.

[1367] Id at 54.

[1368] See NIAC (Singapore) *Report on a Model Data Protection Code* 15-18 [online].

[1369] Litan *Law and Policy in the Age of the Internet* 1 [internet].

government regulation.[1370]

The term "self-regulation" has a range of definitions. As noted by a former US Assistant Secretary of Commerce, Larry Irving,[1371] at one end of the spectrum:

> [T]he term is used quite narrowly, to refer only to those instances where the government has formally delegated the power to regulate, as in the delegation of securities industry oversight to the stock exchanges. At the other end of the spectrum, the term is used when the private sector perceives the need to regulate itself for whatever reason—to respond to consumer demand, to carry out its ethical beliefs, to enhance industry reputation, or to level the market playing field—and does so.

Self-regulation is a model of regulation that works without direct or very minimal government intervention. It is a model of regulation that is much favoured in the US. In 1997 for example, the Clinton Administration declared that "[f]or electronic commerce to flourish, the private sector must lead. Therefore, the Federal Government should encourage industry self-regulation whenever appropriate."[1372]
Under this model of regulation, the industry players initiate and oversee self-regulation by drawing up codes of practice according to the different shades of activity in the industry.[1373] The main advantages of self-regulation are said to include efficiency, increased flexibility, increased incentives for compliance and reduced cost.[1374] It is argued on behalf of self-regulation that because of their proximity to the members of an industry group, self-regulating members in an industry are likely to have superior knowledge of the industry and the subject matter of the regulation than a government agency.[1375] In a pure sense, self-regulation concerns private actors

---

1370 Strauss and Rogerson 2002 (19) *Telematics and Informatics* 181.

1371 Irving *Privacy Report* [online].

1372 Clinton *Presidential Directive on E-Commerce* [online]. Also, the Federal Trade Commission, the American agency with greater responsibility for privacy in the marketplace, has largely been in favour of self-regulation. For example, in the Commission's Report to Congress in July 1999, the Commission stated that "self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology." See FTC *Self-regulation and Privacy Online* [online].

1373 See n 1368 at Chp 6.

1374 Campbell 1993 (51) *Fed Comm L J* 715.

1375 Michael 1995 (47) *Admin L Rev* 181 – 182.

who make rules for and by themselves on a voluntary basis to address common problems or interests.

As a flexible mode of regulation, it is argued that self-regulation makes it easier for trade associations or industry groups to change their rules when necessary than for governments to amend their regulations.[1376] Another argument is that self-regulation provides greater incentives for compliance.[1377] If rules are developed by the industry, it is argued, industry participants are more likely to perceive them as reasonable and therefore acceptable. Companies are more willing to comply with rules developed by their peers than by outsiders such as government agencies.[1378]

4.2.1 Arguments against self-regulation.

One of the strongest arguments against self-regulation is that it creates the opportunity for the industry to subvert the regulatory objective to its own business profit goals.[1379] According to Swire,[1380] it is doubtful whether companies will use their expertise to the benefit of the public. Rather, he suggests, they are more likely to employ their expertise to maximize the industry's profits.

Another strong argument against self-regulation is that the self-regulated industry may not have the necessary coercive power to enforce the self-regulating codes of practice; at most, an industry group may expel a member for non-compliance but that is not incentive enough for the others to abide by the code of practice. It is argued that where a company is likely to make more profit by ignoring self-regulation, it is more likely to do so.[1381] Self-regulatory frameworks can simply unravel because of cheaters.[1382]

While self-regulation is not altogether bad, it has largely been seen to be ineffective

---

[1376] Ibid.

[1377] Id at 183-184.

[1378] Swire "Markets, Self-Regulation and Government Enforcement" [online].

[1379] Baker and Miller "Privacy, Anti-Trust and the National Information Infrastructure" [online].

[1380] See n 1375.

[1381] Ibid.

[1382] Perritt "Regulatory Models for Protecting Privacy" [online].

in achieving the aims of the codes of self-regulation.[1383] The two greatest weaknesses of this approach to regulation are inadequacy of the codes and their lack of or weak enforcement. Because it usually involves a heterogeneous collection of industry members, this heterogeneity makes self-regulation, particularly the adequacy of the codes and their enforcement, very hard to achieve.[1384] The consequence is the lowering of protection standards. Compared with the higher standard set by comprehensive statutory regulation as exemplified by the EU's *Directive*, self-regulation, particularly outside the US, is deemed to be inadequate. The problems associated with self-regulation such as lack of enforceability, redress, and punishment make the model less than ideal for meeting one of the fundamental goals of regulatory authorities which is to achieve compliance with the regulations embodied in a regulatory regime.[1385]

While critics maintain that government intervention creates burdensome and inflexible regulation and self-regulation fails for lack of enforceability, the apparent success of the EU *Directive* invites attention to the necessity of government involvement in regulation. According to Hirsch,[1386] European nations have in recent years developed a third approach to privacy protection which provides a way for government and industry to work together to create and enforce a set of privacy rules.

According to Hirsch, the European model is not self-regulation since the government retains an important role in reviewing and approving the proposed codes of conduct.[1387] But neither is it pure government regulation since the industry associations, not the regulators, draft the detailed rules and standards that will

---

1383 Paterson 1998 (26) *Fed L Rev* 381.

1384 Scarpa "The Theory of Quality Regulation and Self-Regulation" 236-260.

1385 Abbot 2005 (17) *J Environmental Law* 161–180.

1386 See n 1364 at 7. Hirsch notes that under the European model, the government passes a comprehensive data protection statute that sets broad, flexible, standards regarding the collection and use of personal information. What distinguishes this model from the American self-regulatory model is that rather than the government passing regulations fleshing out these standards, as common with the American regulatory model, they invite the relevant industry sector, acting through its trade association, to draft an industry "code of conduct" that interprets the statute and spells out how it applies to that sector.

1387 Ibid.

govern their members. This model of regulation is known as "co-regulation".[1388]

4.3 Co-regulation

The third model, co-regulation, in which the government and industry jointly regulate data protection, is favoured in Australia and Canada.[1389] Co-regulation refers to regulatory regimes where non-state actors and the state collaborate to introduce or enforce regulatory solutions. Industry-wide standards are defined and enforced through legislative endorsements of a code of practice. The industry or self-regulatory organisation undertakes to achieve the regulatory objectives stipulated by the state. Co-regulation represents an intermediate strategy between a model of pure self-regulation and a model of rigid state command and control regulation.[1390]

Under a co-regulatory regime, the regulatory role is shared between the private sector and the state. According to Ayres and Braithwaite,[1391] a co-regulatory regime is based on a tripartite structure which can occur in a more or less formal manner either directly through state intervention or through the participation of interest groups in negotiations. Under a co-regulatory regime, the state may be responsible for approving the self-regulatory measures and rules applying to an industry and which are then implemented by the regulated industry. The state will be responsible for exercising some on-going oversight and may also assume some enforcement functions. The level of government involvement in a co-regulatory model varies from little control to more significant intervention by government.

4.4 Conclusion

Whatever the model of choice, it is pertinent to note that the existence of an independent data protection authority is generally regarded as a prerequisite for an

---

1388 Ibid. See also Hans-Bredow Institut *Final Report* 11-16 [online]; Harter 2009 *J Disp Resol* 411.

1389 Hong Kong, New Zealand, Canada and Australia are some of the countries operating co-regulatory regimes where statutes are complemented by industry self-regulatory codes. See National Internet Advisory Committee (NIAC) (Singapore) *Report on a Model Data Protection Code for the Private Sector* 15-18 [online].

1390 Senn *Non-state Regulatory Responses: Understanding Institutional Transformation* 140.

1391 Ayres and Braithwaite 1991 (16) *L & Soc Inquiry* 439; see also Grabosky and Braithwaite *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies* 83.

adequate data protection regime. Article 28 of the EU *Directive* requires member countries to have an independent supervisory authority. Countries looking to secure the EU's certification of "adequate" data protection regime must have regard to the establishment of an independent national data protection authority. The better a regulatory regime conforms to the EU template, the better that regime's chances of being adjudged adequate.

The trend in a significant number of the countries that have enacted data protection laws is toward some form of an omnibus or comprehensive data protection regime. Establishing regulations and incentives for compliance, as well as consequences for privacy violations is very critical for the success of any data protection regime. The current practice in those countries with data protection laws is that oversight of data protection laws usually rests in the hands of national data protection authorities which are headed by either "privacy commissioners" or "information commissioners."

Data protection authorities (DPAs) are independent government agencies established to protect privacy and oversee compliance with data protection laws. They are generally responsible for the enforcement of national data protection laws and they typically have the power to hear complaints from individuals, investigate data processing activities, impose sanctions (such as fines) and institute civil and criminal proceedings. In many cases, data protection authorities can issue warnings or reprimands, impose fines or order compensation for individuals aggrieved by the wrongful use of their personal data.[1392]

Effective legislation is needed to create and reinforce the power of monitoring/supervisory authorities to ensure compliance and thereby fulfil one of the fundamental goals of regulatory authorities, which is to achieve compliance with the regulations embodied in a regulatory regime. Whether the regulatory model selected is comprehensive in scope or sectorial, there remains the question whether the regulatory regime should be run on general principles or specific rules?

[1392] See OECD *Report on Cross-Border Enforcement of Privacy Laws* 12-16. The OECD Report examined the regulatory and enforcement mechanisms that have been established in countries with data protection laws to resolve consumer complaints and address non-compliance with privacy laws.

5. RULES VERSUS PRINCIPLES

According to Andreas Busch, regulation theory distinguishes between principles-based and rules-based regulation.[1393]

5.1 Rules-based regulation

Regulatory rule-making has until recent times been the predominant mode of regulation. For many years, rules have dominated the regulatory landscape. Regulators and industry players have sought refuge in clear rules because they are thought to be simpler and easier to follow than principles.[1394] In a typical rules-based regulatory setting, agencies of government would issue written rules that inform the regulated business or industry how to conduct their business. The rules would usually specify acceptable and unacceptable behaviour.[1395]

Rules are prescriptive and provide individuals with information about consequences. They promote predictability and precision to the extent that they provide the content of the law before individuals act. Thus, they can result in a determinate legal conclusion that follows the triggering facts.[1396] Prescriptive rules can reduce the level of discretion on the part of individual managers or regulators thus making it less likely for them to be motivated by a desire for personal gain at the expense of the public. On the negative side however, a rules-based approach tends to encourage those regulated to play games with the rules, to find loopholes in the rules, and to find ways around the rules.

5.2 Principles-based regulation

Principles-based regulation generally relies more on high-level, broadly stated rules

---

[1393] Busch 2010 (26) *JPRG* 9.

[1394] Coglianese, Healey, Keating and Michael "The Role of Government in Corporate Governance" 11 [online].

[1395] Morriss, Yandle and Dorchak 2005 (29) *Harv Envtl L Rev* 191-195.

[1396] Sullivan 1992 (106) *Harv L Rev* 58.

or principles to set the standards by which regulated firms must conduct their business.[1397] Unlike the heavy reliance on detailed, prescriptive rules under a rules-based regulatory regime, the principles-based regime sets an overall objective that must be achieved by the regulated bodies. This allows the firms to decide how best to achieve the required regulatory outcomes.[1398] Principles-based regimes are generally seen to be flexible, thereby facilitating innovation and competitiveness. This flexibility assists regulators by providing them with the capacity for regulatory innovation in the methods of supervision adopted. The regulatory regime is thus more durable in a rapidly changing market environment and enhances regulatory competitiveness.[1399] Principles-based regulation is essentially about outcomes or ends while rules based regulation is about means. As noted by Prof. Black, principles provide the framework in which firms can organize their own processes to achieve the outcomes the regulator seeks.[1400]

For the Australian Law Reform Commission for example, a key reason why principles-based regulation is their preferred regulatory model is that it does not prescribe detailed steps that must be complied with, but rather sets an overall objective that must be achieved. According to the Commission, "[a] key advantage of principles-based regulation is its facilitation of regulatory flexibility through the statement of general principles that can be applied to new and changing situations."[1401]

An essential distinction of principles-based regulation is that it is outcome-oriented. An outcome-oriented approach is one in which the regulator devolves decision making over detailed process to the regulated entity. It focuses on the results of enforcement and provides context-sensitive, flexible, dialogue-based ways and techniques to translate those principles into specific business conduct expectations.[1402] The best known principles-based regulator is the Financial Services

---

[1397] Black, Hopper and Band 2007 (1) *LFMR* 191.

[1398] Ibid.

[1399] Black "Forms and Paradoxes of Principles Based Regulation" 3 [online].

[1400] Ibid.

[1401] ALRC *For Your Information* 235 [online].

[1402] See Ford 2010 (2) *Wis L Rev* 457.

Authority (FSA) in the United Kingdom. It provides a list of high-level principles or obligations that firms must fulfil in order to stay compliant.

To achieve the defined principles, businesses must adopt best practices. In acknowledging this approach, the FSA's objective is to focus on the desired outcomes (the principles), and evaluate how well a company manages the risks associated with those principles. Individual companies decide how to meet these principles, and avoid or mitigate risks that will negatively impact them. The focus shifts from the means, to the end.[1403] However, principles-based regulation is not without its disadvantages. It is criticised for failing to provide certainty and predictability, and for creating a regulatory regime in which regulators can act retrospectively. For example, in a letter to the head of the Financial Services Authority in the UK, the Chairman of the Regulatory Law Committee of the City of London Law Society expressed apprehension about the "unacceptable vagueness for firms as to how to satisfy" a financial regulator applying this approach.[1404]

According to Peter Wallison,[1405] principles-based systems are extremely difficult to administer consistently over time, thereby leading to differences in treatment that can have competitive effects. He argues that whether a particular way of doing business conforms to the principle involved can be a matter of a particular regulator's opinion, and as regulators and circumstances change, so do interpretations. An activity previously disapproved can become acceptable - and vice

---

1403 The Financial Services Authority (FSA) was established by the Financial Services and Markets Act 2000, as an independent non-governmental body with statutory powers to regulate the financial services industry in the UK. The primary objectives of the Authority are to enhance market confidence, consumer protection, financial stability and the reduction of financial crimes. The FSA formulated 11 Principles of Business in 2001. Some of its core business principles are:

- A firm must conduct its business with integrity.
- A firm must maintain adequate financial resources.
- A firm must pay due regard to the interests of its customers and treat them fairly.

The Principles do not give specific instructions for how to comply with each principle, but they are objectives all businesses must meet. In June 2010, the UK government disclosed its intention to split the FSA into two new successor bodies, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA). In April 2013, the new successor regulatory bodies came into existence. For more information on the new 'twin peaks' regulatory model of the financial industry in the UK, see the old FSA website [online]. The Principles are now enforced by the FCA and are contained in the FCA *Handbook* [online].

1404 Mortgage Introducer *Law Society Critical of Principle-Based Approach* [online].

1405 Wallison *Fad or Reform* [online].

versa. On the contrary, the existence of detailed written rules under a rules-based regime assures that both the regulator and the regulated know what the rules are, despite a change in personnel on either side.[1406]

5.3 What to consider in deciding what model to adopt

A critical issue, in deciding what model to adopt, is the viability and affordability of regulatory agencies, particularly in the African context, where financial and human resources are a constraint. In Nigeria, the tendency is for regulatory agencies to be placed under the supervision or control of a Ministry or Department of State with responsibility for the activities and/or industry under regulation as its domain. While having the regulator inside the Ministry is the cheapest solution, it is also that which is likely to lead to political interference in day-to-day regulatory decisions.

The form of politics which has operated in Nigeria since independence, irrespective of the regime in power, has been characterised as "prebendal politics".[1407] This is defined as an unremitting and unconstrained struggle for possession and access to state offices, with the chief aim of procuring direct material benefits to oneself and one's acknowledged communal or other sectional group. This peculiar political culture of Nigeria, manifested mainly by egregious corruption, has foisted on the country the devastating consequence of political instability and economic mismanagement. According to Ogundiya, the challenge of corruption "is at the core of the crisis of governance and legitimacy, the establishment of a stable democratic order, rule of law, development and the welfare of citizens... and "has remained a major obstacle to national progress in Nigeria."[1408] Arising from this mix is the risk of "regulatory capture" which may be true of the Nigerian state today where politicians dispense political favours and play a critical role in determining the direction of state policy and regulation. Under such a dispensation, it is possible for regulation to be either created at the outset to favour special interest groups or, even if its origins lie in a true concern for market failure, over time it is "captured" by sectional interests

1406 Ibid.

1407 Joseph *Democracy and Prebendal Politics in Nigeria: The Rise and fall of the Second Republic* 55.

1408 See Ogundiya 2009 (11) *Anthropologist* 287.

intent on promoting their own economic interests.[1409]

When it comes to designing or adopting a regulatory framework for data protection, it is useful to bear in mind the argument of Rachel Greenstadt and Michael D. Smith,[1410] that the practicality and utility of any approach to protecting personal information depends critically on how the approach addresses the issues of decision-making, negotiation, and enforcement.[1411] In regard to decision-making, it is necessary to know who the decision-makers are and whether they have the right information and incentives to make good decisions about what personal information is worth protecting and controlling.

Negotiation is the process by which data subjects and data users reach agreement on the rights and responsibilities of the data users with respect to the data subjects' personal information. The result of negotiation should be a clear statement describing the rights and responsibilities of the data user with respect to an individual's personal information.

Enforcement is the mechanism or set of mechanisms that provide a guarantee that the data user abides by the negotiated rights. A good enforcement mechanism should be judged in terms of strength and transparency. A transparent mechanism is one in which the data subjects are allowed to see who had or still has access to their released personal information.[1412]

A key question to answer in deciding the type of regulatory model to adopt is whether the objectives/functions of the regulatory institution are clearly defined? Resolving this issue is crucial in order to avoid the problem of regulatory overlap that is common under the present arrangement where regulatory agencies of government are routinely carved out of ministerial departments without clear objectives and the

---

1409 See Minogue and Carino *Regulatory Governance in Developing Countries* 11-12, who argue that "political capture" is a form of regulatory capture under which certain legislative and contractual arrangements are deliberately designed and promoted to meet the needs of the political elite. See also Stigler 1971 (2) *Bell J Econ Manag Sci* 3-21; Posner 1974 (5) *Bell J Econ Manag Sci* 335-58; Peltzman 1976 (19) *JL & Econ* 211-240.

1410 Greenstadt and Smith *Protecting Personal Information* [online].

1411 Ibid at 5.

1412 Id at 6-8.

statutory mandates of different regulatory authorities contradict one another.[1413] The problem of regulatory overlaps and statutory inconsistencies make it clear that deciding what model of regulation to adopt will not be an easy decision to take.

[1413] A good example of regulatory overlap arising from inconsistent statutory provisions is the flexing of regulatory muscles by the Nigerian Communications Commission (NCC) and the National Environmental Standards and Regulations Enforcement Agency (NESREA) over the location of a telecommunications company's base transmission station. Although the law setting up NCC gives it overwhelming powers to regulate the telecoms sector, the NESREA Act, 2007 in s 7 empowers it to enforce "… environmental standards, regulations, rules, laws, policies and guidelines" even in cases involving telecommunications companies with regard to their infrastructural activities to the extent that they impact the environment.

NESREA had sealed the premises of MTN's base transmission station at EFAB Estate, Mbora District in Abuja. NCC unsealed the station, after which NESREA went back to seal the base station again and slammed a fine of N5 million on MTN for reopening its base station. This was clearly a case of inter-agency rivalry between the NCC and the NASREA over the regulation of telecoms infrastructure. The NCC Act, 2003 provides in s 136(3) that "All licensees shall in connection with installation of their respective network facilities take all reasonable steps to protect the safety of persons and property, ensure that the activity interferes as little as practicable with the use of land and environment." On the other hand, the NESREA Act 2007 provides in s 2, "The agency shall be the enforcement agency for environmental standards, regulations, rules, laws, policies and guidelines." Needless to say, that the clash was an embarrassment to the government. See Obi 3rd May 2012 *Thisday* [online].

CHAPTER 9

CONCLUSION, SUMMARIES AND RECOMMENDATIONS

1. CONCLUSION

In the last two decades, there has been a shift in public policy away from state ownership and state provision of services, to private ownership and private provision of services. This has come at the expense of greater state regulation; it has resulted in what Majone[1414] describes as the rise of the "regulatory state". In this new dispensation of governance, the state ceases to be directly concerned with the provision of goods and services and instead concentrates upon regulating private markets and its operatives in order to promote economic and social welfare.

Even though the developing countries of Africa have historically had little interest in privacy policy, they are increasingly finding that such policy interest is forced upon them by external factors. The European Union's *Data Protection Directive* is a key factor. Countries that wish to maintain good trade relations with the European Union, and encourage the flow of foreign direct investment into their territories, are finding themselves obliged to conform to Europe's requirements for adequate data protection. Argentina was one of the earliest countries outside the EU to introduce comprehensive legislation along European lines. Since then, other countries have followed suit. It will therefore not be uncommon for Nigeria to take the same steps by enacting a data privacy regulatory regime. The faltering steps taken so far in formulating a workable data protection regime in the country clearly indicate the need for a broad-based consultative approach to data protection legislation in view of the country's socio-cultural ethos.

[1414] Majone 1994 (17) *W Eur Pol* 83-88. He traces the rapid growth of administrative regulation in Europe by means of agencies operating outside the line of hierarchical control or oversight by the central administration. (p 83).

In choosing a regulatory model for data protection in Nigeria, it is important to recognise that any regulatory institution that will be established will be set up in an existing governance/regulatory environment and must therefore operate within the dynamics and constraints influenced by existing institutions and systems. The governing environment under which the new regulatory institution will function has itself been fashioned by long-standing values, attitudes and traditions of behaviour that do not easily lend themselves to change.

The socio-cultural ethos of Nigeria has in the last forty years been greatly influenced by a military world-view that paid scant attention to the rule of law. Governance was largely characterised by the command and control model of governance. The constitutional distribution of powers was irrelevant under the military regimes that have predominantly ruled Nigeria. The legislative powers of the military governments of the past were unlimited, with no legally prescribed procedure for law-making.[1415] The political system in the country, whether military or civilian, has usually been based on patronage while rent collection remains an important element in the regulation of the Nigerian economy in general.[1416] According to Lewis, the political allotment of economic gains and the corruption that accompanies state patronage generally creates adverse economic conditions. Collusion between state officials and private clients give rise to inefficiency, capital flight, inequality, widespread mistrust and uncertainty.[1417]

This political culture and the legislative nature of the military regimes of the past have given rise to "a highly personalised topology of the rules and regulations"[1418] in the Nigerian economy. It is fairly safe to assert that despite the change from military authoritarian rule to a democratic dispensation, the prescriptive model of governance continues to dominate the regulatory environment in Nigeria.

Any proposal for regulatory intervention for the protection of information privacy in

[1415] See Nwabueze *Military Rule and Constitutionalism* 8.

[1416] See Lewis *Growing Apart: Oil, Politics, and Economic Change in Indonesia and Nigeria* 6.

[1417] Ibid.

[1418] See Okigbo *Essays in the Public Philosophy of Development Vol 3: Growth and Structure of the Nigeria Economy* 258-259.

Nigeria must be formulated within the context of the interactions between politics and economics. A neglect of this reality may doom any regulatory proposal to failure. In arguing for the enactment of a data protection law in Nigeria, it is understood that such a proposal will raise various questions and concerns. Firstly, the question of whether the proposed law should apply to the government, (including state and local governments) and the private sector must clearly be determined. Obviously the governments, federal, state and local, through their various statutory agencies, are the largest collectors and custodians of personal data in the country. Excluding them from the ambit of a data protection law would undermine the objectives of such a law. The private sector is also a very significant collector of personal information and would naturally be a major focus of regulatory supervision. The proposed legislation earlier considered clearly misses the mark by excluding data held by government from the ambit of the proposed law.

Other relevant questions include whether there should be exemptions in the application of the law, particularly in relation to crime investigations, national security, the Freedom of Information Act and health records. Questions relating to transactional costs and cross-border effects in relation to other countries will also have to be considered.[1419] There is also the challenge of setting jurisdictional limits - which organ of government enforces the law – the courts or the Privacy Commissioner where the law creates such an office, or the private sector?

In conclusion, the choice of regulatory infrastructure is not determined by hard and fast rules set in stone. Each country must work out what best suits its peculiar needs and circumstances based on its level of development. As noted by Srivastava, "there is no unique design of regulatory institutions that can be transplanted from one country/sector to another."[1420] The successful regulatory institution would be the one that constantly adapts to its changing environment and regularly evaluates the effectiveness of its methods and decisions.[1421] It remains to be said that an effective regulatory infrastructure supports a country's economic development and the rule of

[1419] See Mellors and Pollitt 1984 (37) *Parliamentary Affairs* 206-207.

[1420] Srivastava *Issues in Institutional Design of Regulatory Agencies* [online].

[1421] Ibid.

law. It helps the government to take the right decisions about what to regulate, whom to regulate, and how to regulate.

2. SUMMARIES

As suggested by its title, this thesis set out to study the role and impact of trans-border data flows and data protection laws from other countries on Nigeria's quest for integration into the global network economy.

The global market network that Nigeria seeks to connect to is a flexible inter-connected system centred on multinational corporations, global financial markets and a highly concentrated system of technological research and development.[1422] The global market network links up everything that is valuable according to dominant values and interests, but disconnects everything that is not valuable, or becomes devalued.[1423]

Being an active member of the global network economy is essential to Nigeria's economic growth. To succeed in the twenty-first century, Nigeria has to become a full partner in the global network economy. It must plug into the network or risk being shut out. The global market network operates by means of rules and standards that are largely set by the dominant players in the network who demand adherence by those who seek to interact with it. Data protection is a critical component of the regime of rules and regulations that govern the global network economy; it is evolving into an emerging legal order that transcends geographical boundaries.

The EU *Directive* on data protection is the *de facto* global standard for data protection and has put data protection and the notion of human rights in the mainstream of international trade.[1424] One reason for its ascendancy is the threat implicit in the *Directive*, to exclude non-EU countries that fail to comply with the standard set for data protection in EU member countries.

[1422] See chp 7 par 2.1.

[1423] Ibid.

[1424] Heisenberg and Fandel *Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard* 109-129.

The *Directive* has given rise to an international harmonisation of domestic data protection laws whereby countries outside the EU are more or less compelled to enact data protection laws that approximate to the standard set by the EU *Directive*. This trend provided a compelling reason for examining the issues relating to privacy and data protection[1425] in Nigeria as the country seeks to integrate into the global network economy.

In Nigeria, the tension between privacy and freedom of information takes place against the backdrop of an endemically corrupt society in desperate need for solutions to the malaise. The pressure to restore the international community's confidence in Nigeria, particularly its commercial activities, presents (to the government) the temptation to "cut corners" in achieving that objective by not strictly observing the rules in law enforcement and crime detection efforts. In such an environment, privacy interests are greatly at risk.

The news media and the security agencies are concerned that the restrictions that a vigorous privacy regime would impose, could undermine freedom of information and expression and inhibit the discovery and disclosure of the truth. The right to privacy is not inferior to any other right and should not be seen as something sought by criminals or deviants in order to hide shameful conduct or corrupt practices. It is a right guaranteed under the Nigerian constitution.

The question arose whether the constitutional guarantee of privacy also includes data protection and if it does, whether the protection is adequate in the light of current global trends in data protection enactments. To answer the question, a careful examination of the current state of data protection in Nigeria and its adequacy was undertaken in chapter 7.[1426] While there is at present, no omnibus privacy or data protection law in Nigeria, personal data is protected to some extent by a number of statutes; these statutes have limited scope and application. There is need for a more comprehensive data protection as acknowledged in the country's IT Policy. The Policy recognises the need to "promote legislation (Bills and Acts) for the protection

[1425] See chp 1 par 2.1.

[1426] See par 3.4

of on-line business transactions, privacy and security" and to "enhance freedom and access to digital information at all levels while protecting personal privacy".[1427]

It was also found that the statutory protection of privacy is more concerned with securing the confidentiality of information collected by the government and its agencies. The extant statutes do not address private sector collection, processing and storage of personal information. The reference to correspondence, telephone conversations and telegraphic communications in the constitutional guarantee of the right to privacy evinces a clear intention to protect information privacy. This intention is however not borne out by a significant body of case law of information privacy protection or a robust data protection advocacy.

The study found that key sectors of the Nigerian economy have migrated their activities and data to the Internet. These sectors, such as oil and gas, financial services and telecommunications, are critical sectors of the country's national economic and security interests. Computer systems and networks running those sectors constitute critical information infrastructure. Their impairment would have a negative impact on the overall economy and well-being of Nigerian citizens. In addition to the growing reliance on ICTs and the Internet, there is a growing mass of customers subscribing to online services offered both by the financial and telecommunications companies in Nigeria. This proliferation of business activities in relation to customer information demands that customers' personal data should be protected.

There are no legal guidelines as to how customers' personal information should be used or disposed of. Banks, financial institutions and telecommunications companies have accumulated a lot of personal information about their customers and though some measure of direction has been given by the Central Bank of Nigeria to the financial industry on how to deal with customers personal data, there remains no purposeful protection of customers' personal data.

Nigeria's bilateral and multilateral obligations arising from conventions or other treaties it has signed obligate it to update its legal system to meet global standards. For example, Article 39 of the *TRIPS* Agreement makes provision for the protection

[1427] See n 1228.

of personal data submitted to governments or governmental agencies against disclosure without the consent of the owner of the information.[1428] The article clearly envisages a national data protection regime in WTO member states that will protect personal data as well as pharmaceutical, agrochemical and traditional medicine-related data against disclosure and unfair commercial use by third parties.[1429]

Nigeria needs a data protection law not only to protect the privacy rights of Nigerian citizens, but also to hold all collectors and users of personal data, including cyber criminals, responsible for their wrongful dealings with private data. A well-crafted data protection law should protect the interests of not only Nigerians, but every person resident in Nigeria.

A data protection law in Nigeria will regulate and thereby facilitate the use of personal data by all operators in the marketplace in an environment that will greatly reduce the incidence of abuse. It will impose discipline over a new breed of Nigerian information technology professionals who are yet to be regulated by any enforceable code of ethical behaviour in relation to their handling of personal data.

The absence of a data protection regime is a significant business and social engineering deficit in Nigeria. The EU is a very significant block of Nigeria's trading partners and bearing in mind the stringent requirements of the EU *Directive*, there is need for legislative intervention to protect private data. It is important that Nigeria's privacy laws keep pace with international norms in order to facilitate international trading opportunities. It is equally important that Nigeria, as a developing country, is able to stay relevant, by continuing to play on the international stage. This will be effective only if its systems and protections have the same integrity as those in other countries, particularly its larger trading partners. In an era of increasing globalisation and e-commerce, Nigeria's inability to give this assurance is a potential impediment to trade which the country can ill afford.

The South African Law Reform Commission (SALRC) identifies international trade as a primary motivation in seeking the enactment of data protection laws that fit the

[1428] See chp 7 par 4.3.2

[1429] Ibid.

EU standard. The SALRC noted that privacy is an important trade issue that can create a barrier to international trade. It noted that data protection legislation will ensure South Africa's future participation in the information market, "if it is regarded as providing "adequate" information protection by international standards."[1430]
A key element of data protection laws is the regulation of the transfer of personal data to other jurisdictions for processing or use. The flows of financial resources and information across borders has resulted in regulatory spill-overs having consequences both for policy inter-dependence and for the role of the state.

Nigeria's foremost trade competitor in Africa, South Africa, has resolved to adopt a comprehensive data protection regime structured on the EU *Directive*'s principles. The SALRC acknowledges that such a move would raise obstacles when trading with African countries.[1431] This fact ought to be a strong motivation for Nigeria to do the same.

Having argued vigorously that there are compelling reasons for strengthening the protection of information privacy in Nigeria, the study considered what model of regulation should be adopted. Three main models of regulation were examined:

i. Government regulation

ii. Self-regulation

iii. Co-regulation

Proponents of government regulation argue that the desire for profits, coupled with the economic value of personal information, will prevent private firms from taking adequate steps to protect personal data. They therefore seek the government's active intervention by way of legislation that would take a strong stand in protecting personal information.

Self-regulation is a model of regulation that works without direct or very minimal government intervention. Under this model of regulation, the industry players initiate and oversee self-regulation by drawing up codes of practice according to the

[1430] South African Law Reform Commission *Privacy and Data Protection* (Discussion Paper 109) vi.

[1431] Ibid at par 7.2.4(b).

different shades of activity in the industry.

A third approach to privacy protection provides a way for government and industry to work together to create and enforce a set of privacy rules. Co-regulation refers to regulatory regimes where non-state actors and the state collaborate to introduce or enforce regulatory solutions. Industry-wide standards are defined and enforced through legislative endorsements of a code of practice. The industry or self-regulatory organisation undertakes to achieve the regulatory objectives stipulated by the state.

The European model of data protection regulation is co-regulation[1432] because the government retains an important role in reviewing and approving the proposed codes of conduct.[1433] It is not pure government regulation since the industry associations, not the regulators, draft the detailed rules and standards that will govern their members.

Regulation theory distinguishes between principles-based and rules-based regulation. Regulatory rule-making has until recent times been the predominant mode of regulation. For many years, rules have dominated the regulatory landscape. Regulators and industry players have sought refuge in clear rules because they are thought to be simpler and easier to follow than principles.

Rules are prescriptive and provide individuals with information about consequences. They promote predictability and precision to the extent that they provide the content of the law before individuals act. Thus, they can result in a determinate legal conclusion that follows the triggering facts.

On the negative side however, a rules-based approach tends to encourage those regulated to play games with the rules, to find loopholes in the rules, and to find ways around the rules. Principles-based regulation generally relies more on high-level, broadly stated rules or principles to set the standards by which regulated firms must

[1432] See n 1361.

[1433] See n 1358.

conduct their business.[1434]

According to the Australian Law Reform Commission, "[a] key advantage of principles-based regulation is its facilitation of regulatory flexibility through the statement of general principles that can be applied to new and changing situations."[1435]
Principles-based regulation is criticised for failing to provide certainty and predictability, and for creating a regulatory regime in which regulators can act retrospectively. Principles-based systems are difficult to administer consistently over time, thereby leading to differences in treatment that can have competitive effects. On the contrary, the existence of detailed written rules under a rules-based regime assures that both the regulator and the regulated know what the rules are, even when there is a change in personnel on either side.

The viability and affordability of regulatory agencies, particularly in the African context where financial and human resources are a constraint, is a critical issue to consider in deciding what model to adopt. In Nigeria, the tendency is for regulatory agencies to be placed under the supervision or control of a Ministry or Department of state with responsibility for the activities and/or industry under regulation. While this option may be the cheapest solution, it is also that which is likely to lead to political interference in day-to-day regulatory decisions.

The form of politics which has operated in Nigeria since independence, irrespective of the regime in power, has been characterised as "prebendal politics"[1436]. This is defined as an unremitting and unconstrained struggle for possession and access to state offices, with the chief aim of procuring direct material benefits to oneself and one's acknowledged communal or other sectional group. This peculiar political culture has foisted on Nigeria the devastating consequence of political instability and economic mismanagement.

[1434] See n 1494.

[1435] See n 1398.

[1436] See n 1404.

3. RECOMMENDATIONS

The study proceeded on the premise that to be a meaningful participant in the global network economy, each nation must agree to abide by the emerging norms and rules that govern interaction within the global network in order to minimise conflicts and maximise benefits. To achieve this, each nation must put in place within its own national jurisdiction, a legal framework that is supportive of the new and evolving legal order and its norms, from which the network economy is expected to derive its legality, certainty and continuance. It is accepted that different nations have different conceptions of privacy and how it should be protected. Nevertheless, harmonisation between information privacy laws is needed in order to allow free flow of information between different jurisdictions.

In the light of the findings made in this study, the following recommendations are made in the hope that Nigeria will not only step up its protection of privacy as guaranteed in the 1999 Constitution, but will also take the crucial step of assuring its trading partners that it is willing to meet the terms of engagement set by the global network economy.

3.1 Enact a comprehensive data protection law based on "fair information principles"[1437]

This study has argued vigorously that in order for Nigeria to realise its Vision 2020 ambitions, particularly in relation to becoming the preferred international trade hub in Africa, the country must meet the data privacy expectations of its current and

[1437] The proposed law will be judged in the light of content principles that specify minimum requirements for the protection prescribed in the regime for it to be judged as adequate. The EU's Working Party on data protection has identified nine content principles that should be embodied in an adequate data protection law:

- the purpose limitation principle;
- the data quality and proportionality principle;
- the transparency principle;
- the security principle;
- the rights of access, rectification and opposition; and
- restrictions on onward transfers.
- special handling of sensitive data;
- possibility to 'opt-out' from direct marketing; and
- special rules for automated individual decision making.

See n 1217.

potential trade partners abroad. It is necessary for Nigeria to improve its international competitiveness and thereby create opportunities for its businesses to fully participate in international trade.

Enacting a data protection law will contribute to the country's competitive edge by assuring Nigeria's international business partners that their citizens' personal information will be protected in Nigeria. This in turn will facilitate the smooth transfer of data between, for example, EU member countries that make up a very significant global market block and Nigeria.[1438] The various states that have enacted data protection laws have converged around a common set of "fair information principles" which form the basis of all data protection law. It is recommended that the proposed data protection law for Nigeria should also reflect the core data protection principles distilled from international documents such as the Council of Europe *Convention No 108* of 1981,[1439] the OECD Guidelines of 1980[1440] and the UN *Guidelines* of 1990.[1441]

It is recommended that the proposed law should make provision for the regulation of trans-border flows of data. It should be noted that the hallmark of the EU *Directive* and the compelling factor in moving other countries to enact similar data protection laws is the restriction it places on the transfer of personal data from the EU to third countries without adequate data protection laws. Nigeria should take a cue from South Africa and impose trans-border data flow restrictions on data transfers to countries without adequate data protection. Without such a restriction and the other recommendations made below, it is hardly expected that when the law is eventually passed, it will receive the stamp of adequacy from the EU.[1442]

[1438] While Article 25 of the EU Directive prohibits EU nations from transferring personal data to third countries which do not guarantee adequate protection of such data, it may also be the case that a third country, not a member of the EU, may restrict onward transfers of data to Nigeria as a result of that third country's data protection law which meets the EU standard.

[1439] See n 1219.

[1440] See n 1220.

[1441] See n 1221.

[1442] For example, the Article 29 Data Protection Working Party noted that Section 5 of the Australian Privacy Amendment (Private Sector) Act *2000* on the extra-territorial operation of the Act applies only to Australians and does not extend the protection of National Privacy Principles (NPP) 9 to non-Australians. "This means that an Australian company can import data from European citizens and subsequently export it to a country with no privacy laws without the Australian Act applying. Such a measure would make it

3.2 Establish a statutory data protection regulatory authority

It is recommended that a statutory data protection authority for enforcing the protection of data privacy be established in Nigeria. This regulatory authority will be responsible not only for enforcing the data protection law, but also complement and strengthen the legal regime by informing and educating the public about their rights in relation to their personal data. It will also provide readily identifiable processes by which complaints from the public may be investigated and settled either within or outside the judicial system.

It is important that the data protection regulatory authority is given the appropriate material and human resources, and adequate enforcement jurisdiction to ensure compliance with any enacted data protection legislation. If adequately resourced, the authority will, depending on the specific regulatory model adopted, help to enforce privacy legislation by providing expert advisory and supervisory services; negotiate and approve codes and standards of practice; impose penalties on violators and where necessary, prosecute them. The regulatory authority must stay ahead of the regulated entities by researching new technologies and developing appropriate measures to adapt the law to changing realities.

Enforcement is a key component of any regulatory regime. As noted by Veljanovski,[1443] it is the enforcement of legal rules that shapes the incentives and deterrents that attempt to alter the behaviour of those regulated and thereby induce compliance with the law. A reading of some of the literature on enforcement shows that economists, political scientists, sociologists and legal scholars have identified deterrence and compliance enforcement strategies as the most effective enforcement

---

possible to circumvent the EU Directive, if Australia was recognised as providing adequate protection." On the basis of the above, the Working Party in its opinion on the Australian Privacy Amendment (Private Sector) Act 2000, considered "that data transfers to Australia could be regarded as adequate only if appropriate safeguards were introduced to meet the above mentioned concerns". (Underlining supplied). In effect, full certification of adequacy was denied because of the inadequacy of protection for extra-territorial transfer of personal data to and from Australia.

See European Commission Article 29 Data Protection Working Party *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*.

[1443] See Veljanovski "The Economics of Regulatory Enforcement" 171.

model.[1444] However, the choice of which enforcement model to adopt in the particular circumstance of Nigeria should be guided by the characteristics of the regulated society. This calls for further investigation by the Nigerian Law Reform Commission and/or other agencies to determine the most effective data protection regulatory enforcement model to adopt.

3.3 Education and publicity: The public must be empowered to take action to protect their personal information.

Privacy is a fundamental human right. Nigerians should be made aware of the privacy protection in the Constitution and the data protection legislation, data protection regulatory authority and its processes when eventually enacted and established. One of the functions of privacy, according to Westin, is to protect the individual from improper surveillance and shield those institutions such as the press, which operate to keep the government accountable.[1445] Privacy is protected in many countries of the world and is the subject of a number of international covenants and human rights treaties.[1446] However, the notion of privacy is weak in the African conception of human rights. Privacy is not recognised as a human right in the *African Charter on Human and People's Rights* which was adopted in 1981.

The literacy level in Nigeria is low, with the result that many are precluded from enjoying the benefits of modern communication and insisting on their rights. With this background, it is easy to see why there is such paucity in the case law on the constitutional guarantee of privacy. Even today, with the improved access to telecommunications facilities, the average Nigerian user of communication facilities

---

[1444] See Abbot 2005 (17) *J Environmental Law* 162; According to Abbot,

> Where a violation is detected, regulators can facilitate compliance by utilising a range of formal and informal administrative tools and sanctions, criminal prosecution and civil litigation. Businesses are more likely to comply with their legislative responsibilities when the regulator has what has been referred to as an 'enforcement pyramid' as opposed to only one deterrence option.

See also Hawkins *Environment and Enforcement: Regulation and the Social Definition of Pollution* 205; Hutter *Compliance: Regulation and Environment*.

[1445] Westin *Privacy and Freedom* at 25..

[1446] Article 12 *Universal Declaration of Human Rights*; Article 17 *International Covenant on Civil and Political Rights*, 1966; Article 8 *European Convention for the Protection of Human Rights and Fundamental Freedoms*, 1950.

is still either ignorant of or indifferent to the privacy implications of the telecommunications technologies.

Education is therefore very crucial in the promotion, realisation and enforcement of human rights. Article 26 of the *Universal Declaration of Human Rights* (UDHR) emphasizes the importance of education in strengthening human rights and fundamental freedoms. Data protection, as an element of the right to privacy will not have room to grow and become established if ignorance continues to be rampant. The government and civil society groups must do more to promote awareness about fundamental human rights and how to access these rights. Education and publicity are critical factors in promoting the citizens' knowledge of their human rights. If data protection legislation is to make any difference in Nigeria, a more robust approach to education and publicity must be adopted.

3.4 Amend section 37 of the 1999 Constitution to make the privacy protection guaranteed therein available to all residents and not only citizens of Nigeria. The data protection law should protect the data privacy of not only Nigerians but all residents in Nigeria including those outside Nigeria whose personal data shall be transmitted to Nigeria.

Section 37 of the 1999 Constitution of Nigeria provides that: "The privacy of citizens, their names, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected." On the face of the provisions of the Nigerian Constitution, only Nigerian citizens have enforceable claims to the fundamental right to privacy since the operative word in the constitutional provision is citizens' either by birth, registration or naturalisation.[1447] Although no court has ruled on this limitation, it is arguable that EU citizens cannot avail themselves of the limited scope of information privacy protection available under the Nigerian Constitution. This limitation of the right to privacy to only Nigerian citizens was first introduced in the 1979 Constitution. Previous Constitutional guarantees of the right to privacy, for example, in the 1960 and 1963 Constitutions, applied to "every

[1447] See n 600.

person".[1448]

The limitation of section 37 of the 1999 Constitution to only Nigerian citizens cannot be justified in the light of the trend towards harmonisation of information privacy rights across several jurisdictions. Every person who is resident in Nigeria should be entitled to the privacy of his home, family and communications. Nigerians resident in South Africa for example, are entitled to the protection of their privacy in respect of their person or home, their possessions and communications.[1449] There is no justifiable reason why a South African citizen or citizen of any other country resident in Nigeria should not enjoy the benefits of the right to privacy. If a data protection law is enacted based on the restricted right to privacy as presently provided for in the Constitution, it would immediately be in danger of failing an adequacy test if it denies data privacy rights to foreigners, particularly EU citizens.

What the EU *Directive* envisages in respect of a third country, is a legal framework consisting of laws and regulations that adequately protect the data privacy of its citizens and therefore able to assure the same protection for EU citizens whose data are transferred to such third country.

3.5 Strengthen the Judiciary

From the information privacy perspective, the most important rationale for establishing a regulatory framework for the digital marketplace in Nigeria is the need to strike the right balance between the protection of the individual's right to his personal and informational privacy and the need to enhance governance, national security and development. The balancing act must also accommodate other service delivery capacities while also facilitating electronic and international commerce through access to personal information. This can best be secured through strengthening regulatory and institutional frameworks and having a robust judicial system. Because of the importance of sound judicial systems to good governance and economic growth, the World Bank and several other donor organizations have

[1448] See s 22 Constitution of the Federation of Nigeria, 1960 and s 23 Constitution of the Federal Republic of Nigeria, 1963.

[1449] See s 14 Constitution of the Republic of South Africa, 1996.

funded judicial reform projects in several developing countries.

Legal, procedural and technical means of ensuring the security of data are imperative if the use of the Internet and e-commerce must flourish in Nigeria. It is needful for the government to play a leading role in fashioning out a legal and regulatory framework for the use of the Internet and e-commerce. This will be accomplished by the enactment of appropriate legislation and regulations to encourage user trust in the system.

The Nigerian judiciary and legal system are largely the products of the colonial era. Some of the substantive and procedural rules of this system are old and in great need of urgent reform. Obsolete rules of procedure cause delays and enforcement challenges. Furthermore, the legacy of long military rule has impacted negatively on observance of and adherence to rule of law and respect for human rights. The current democratic dispensation has not significantly changed the situation.

The legal and judicial processes necessary to give access to those in need of justice are not victim-friendly. There is undue delay in the judicial process which very often leads to denial of justice. The result is that the integrity of the judiciary and the entire legal system is called into question and the uncertainty that results discourages aggrieved persons from pursuing legal remedies. The generally acknowledged corruption in the judicial system[1450] acts as disincentive to investors.

Although the 1999 Constitution safeguards the fundamental human rights of all Nigerians, the fact remains that Nigerians, having suffered for so long under military dictatorship, continue to yearn for their legal system to protect their rights as guaranteed in the Constitution and to provide easily accessible justice which they were denied under military rule. It is therefore imperative that trust be restored in the legal system by way of continuing education of judicial officers and legal practitioners. There is also need to expose the judicial officers to the constant and rapid advances in ICTs and their impacts on every facet of life in the 21st century.

[1450] See Nigerian Bar Association *Communiqué* [online].

3.6 The Nigerian Law Reform Commission should conduct further studies and carry out extensive consultations with all stakeholders in the society in order to determine the best regulatory model to adopt.

It is hoped that when eventually a data protection law is enacted in Nigeria, it would cover all persons and institutions such as employees, customers, clients, members of organizations or societies, patients, citizens, legal residents, suppliers, business associates and all other collectors of information relating to individuals. The law will inevitably engender fundamental changes to current policies and practices relating to the collection, holding, processing, use and disclosure of personal data. Such policies and practices will have to be re-examined and new ones will have to be put in place to ensure compliance with global demands. Current personal perceptions about the value of personal data and the potential for abuse of such data will also have to change.

This thesis does not pretend to cover every area touched by the trans-border flow of data and their implications for Nigeria's integration into the global network economy. The scope of the study has been limited to a broad examination of the impact of trans-border data flows on the protection of information privacy globally and how such impacts affect Nigeria's efforts to connect to the global network economy. The study has recommended the enactment of a data protection law based on the EU standard. However, it is obvious as the study shows, that privacy, to the extent that it seeks to set boundaries between the individual and other members of the community at large, is at odds with the strong communal ethic of African societies.

The fact that traditional African social and political life is primarily communal and hierarchical in structure, calls for further investigation to determine what regulatory model will best suit the peculiar nuances of Nigeria's cultural ethos before a data protection law is enacted. The Nigeria Law Reform Commission, as part of its statutory mandate should initiate a broad-based discussion by all segments of the society to address the issues arising from the widespread use of ICTs in Nigeria and how they affect the privacy of all users of ICTs in the light of the communal ethic of Nigerian societies.

As the second largest economy and largest developing country in Africa, Nigeria is undergoing unprecedented digitisation in personal data processing, in both the public and private sectors. Unregulated automatic and manual data processing runs rampant, particularly in the telecommunications and banking industries. Individuals' right to personal data protection is not guaranteed even though the constitution guarantees the right to privacy. Existing statutory instruments directly and indirectly related to the protection of personal information are incapable of providing adequate data protection for the people in the digital age.

The complexities of the global market network place an enormous burden on Nigeria to establish a regulatory framework in order to operate effectively in the digital marketplace. The fact that a reasonably well functioning legal system is a necessary condition for a country's prosperity cannot be denied. When law is weak or the legal system is in disarray, the enforcement of property, contract and human rights is weak or frequently depends on the threat or actuality of violence and in the long run adds extra costs to the cost of living and of business transactions. This cannot be good for a country that aspires to be one of the biggest global economies by the year 2020.

BIBLIOGRAPHY

BOOKS & JOURNALS

A

Abbate *Inventing the Internet*

Abbate J *Inventing the Internet* (MIT Press 2000)

Abbot 2005 (17) *J Environmental Law* 161

Abbot C "The Regulatory Enforcement of Pollution Control Laws: The Australian Experience" *Journal of Environmental Law* Vol 17 No 2 (2005) 161–180

Ackerman and Sandoval-Ballesteros 2006 (58) *ALR* 85

Ackerman J M & Sandoval-Ballesteros I E "The Global Explosion of Freedom of Information Laws" *Administrative Law Review* Vol 58 No 1 (2006) 85-130

Aihe and Oluyede *Cases and Materials on Constitutional Law in Nigeria*

Aihe D O and Oluyede P A *Cases and Materials on Constitutional Law in Nigeria* (Oxford University Press, 1979)

Ajami 1990 (5) *IJTM* 589

Ajami R "Global Trans-border data flows: Concerns and options" *International Journal of Technology Management* Vol 5 No 5 (1990) 589-604

Al Gore (Vice President's Press release August 6 1999)

Al Gore (Vice President's Press release August 6 1999), quoted in O'Neill M E "Old Crimes in New Bottles: Sanctioning Cybercrime" 9 *Geo. Mason L Rev* 237 (2000-2001) 1

Altman 1977 (33) *J Soc Issues* (1977) 66

Altman I "Privacy Regulation: Culturally Universal or Culturally Specific?" *Journal of Social Issues* Vol 33 No 3 (1977) 66-84

Appadurai *Modernity at Large: Cultural Dimensions of Globalization*

Appadurai A *Modernity at Large: Cultural Dimensions of Globalization* (University of Minnesota Press, 1996)

Arndt 1949 (3) *Aust Q* XXI 68

Arndt H W "The Cult of Privacy" 1949 (3) *Australian Quarterly* XXI 68-71

Ayres and Braithwaite 1991 (16) *L & Soc Inquiry* 435

Ayres I and Braithwaite J "Tripartism: Regulatory Capture and Empowerment*" Law and Social Inquiry* Vol 16 No 3 (1991) 435-496

B

Bacon *Novum Organum*

Bacon F *Novum Organum*, Aphorism 129, quoted in Eisenstein E *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe* (1980)

Baker and Byler 1983 (17) *JWT* 458

Baker J C and Byler E U "SWIFT: A Fast Method to Facilitate International Financial Transactions" 17 *Journal of World Trade* No 5 (1983) 458–465

Baldwin and Cave *Understanding Regulation: Theory, Strategy and Practice*

Baldwin R and Cave M *Understanding Regulation: Theory, Strategy and Practice* (Oxford University Press, 1999)

Banisar 2010 (16) *EAJP&HR* 124

Banisar D "Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information" *East African Journal of Peace & Human Rights* Vol 16 No 1 (2010) 124-154

Barendt *Freedom of Speech*

Barendt E *Freedom of Speech* 2nd ed (Oxford University Press, New York, 2005)

Basu *Global Perspectives on E-Commerce Taxation Law*

Basu *Global Perspectives on E-Commerce Taxation Law* (Ashgate Publishing Ltd, 2007)

Beauchamp *History of Telegraphy*

Beauchamp K *History of Telegraphy* (The Institution of Engineering and Technology 2001)

Bell *The Coming of Post-Industrial Society*

Bell D *The Coming of Post-Industrial Society* (Basic Books 1976)

Bellman, Johnson, Kobrin and Lohse 2004 (20) *Information Society* 313

Bellman S, Johnson E J, Kobrin S J and Lohse G L "International Differences in Information Privacy Concern: Implications for the Globalization of Electronic Commerce" *Information Society* Vol 20 No 5 (2004) 313-324

Bennett and Raab *The Governance of Privacy: Policy Instruments in Global Perspective*

Bennett C J and Raab C D *The Governance of Privacy: Policy Instruments in Global Perspective* (Ashgate Publishing, Ltd., 2003)

Bennett *Regulating Privacy*

Bennett C *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press New York 1992)

Bennett "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?"

Bennett C J "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" 99-123 in Agre P E and Rotenberg M (ed) *Technology and Privacy: The New Landscape* (MIT Press, 1998)

Bergkamp 2002 (18) *C L S Rev* 31

Bergkamp L "The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-driven Economy" *Computer Law & Security Review* Vol 18 no 1 (2002) 31-47

Bermann 1996 (9) *Admin L J Am U* 933

Bermann G A "Regulatory Cooperation between the European Commission and US Administrative Agencies" Vol 9 *Administrative Law Journal of American University* (1996) 933-961

Bignami 2005 (26) *Mich J Intl L* 807

Bignami F "Transgovernmental Networks vs Democracy: The Case of the European Privacy Network" *Michigan Journal of International Law* Vol 26 (2005) 807-868

Black's Law Dictionary

Black's *Law Dictionary* 6th ed (West Publishing Coompany, 1990)

Black, Hopper and Band 2007 (1) *LFMR* 191

Black J, Hopper M and Band C "Making a Success of Principles-based Regulation" *Law and Financial Markets Review* Vol 1 No 3 (2007) 191-206

Blumenthal 1988 (66) No 3 *Foreign Affairs* 529

Blumenthal W M "The World Economy and Technological Change" (66) No 3 *Foreign Affairs* (1987/1988) 529-550

Bovens 2002 (10) *JPP* 317

Bovens M A "Information Rights: Citizenship in the Information Society" *Journal of Political Philosophy* Vol 10 No 3 (2002) 317-341

Boyd and Ellison 2008 (13) No 1 *JC-MC* 210

Boyd D and Ellison N "Social Network Sites: Definition, History, Scholarship" *Journal of Computer-Mediated Communications* Vol 13 No 1 (2008) 210-230

Busch 2010 (26) *JPRG* 9

Busch A "The Regulation of Privacy" *Jerusalem Papers in Regulation and Governance (Working Paper No 26)* (2010)

Bygrave *Data Protection Law: Approaching Its Rationale, Logic and Limits*

Bygrave L A *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Springer, 2002)

Bygrave (2000) *PrivLawPRpr* 7

Bygrave L A "An international data protection stocktake @2000 Part 1: regulatory trends" *Privacy Law and Policy Reporter* 6 (8) (2000) 129

Bygrave 2004 (47) *Sc St L* 319

Bygrave L "Privacy Protection in a Global Context - A Comparative Overview" 2004 (47) *Scandinavian Studies in Law* 319-348

Braga 1996 (33) *Finance & Development* 34

Braga C A "The Impact of the Internationalisation of Services on Developing Countries" 1996 (33) *Finance & Development* 34-37

Braithwaite and Braithwaite 1995 (4) *Soc Leg Stud* 307

Braithwaite J and Braithwaite V "The Politics of Legalism: Rules versus Standards in Nursing-Home Regulation" Vol 4 No 3 *Social and Legal Studies* (1995) 307-341

Brock Foreword to Feketekuty *International Trade in Services: An Overview and Blueprint for Negotiations* (1988)

Brock W E Foreword to Feketekuty G *International Trade in Services: An Overview and Blueprint for Negotiations* (HarperCollins Canada, 1988)

Busch 2010 (26) *JPRG* 1

Busch A "The Regulation of Privacy" *Jerusalem Papers in Regulation and Governance (Working Paper No 26)* (2010) 1-21

C

Campbell 1993 (51) *Fed Comm L J* 712

Campbell A J "Self- Regulation and the Media" *Federal Communications Law Journal* Vol 51 No 3 (1993) 712-772

Casson *The History of the Telephone*

Casson H N *The History of the Telephone* (Echo Library 2007)

Cate *Privacy in the Information Age*

Cate F H *Privacy in the Information Age* (Brookings Institution Press 1997)

Cate and Litan 2002 (9) *Mich Telecomm & Tech L Rev* 35

Cate F and Litan R "Constitutional Issues in Information Privacy" 2002 (9) *Michigan Telecommunications Technology Law Review* 35-63

Cate 2008 (43) *Harv C R-C L L Rev* 435

Cate F H "Government Data Mining: The Need for a Legal Framework" 43 *Harvard Civil Rights-Civil Liberties Law Review* Vol 43 No 2 (2008) 435-489

Catlett "Internet Evolution and Future Directions"

Catlett C "Internet Evolution and Future Directions" chp 19 in Lynch D C and Rose M T (ed) *The Internet Systems Handbook* (Addison-Wesley, 1993)

Cavoukian and Hamilton *The Privacy Payoff: How Successful Businesses Build Customer Trust*

Cavoukian A and Hamilton T J *The Privacy Payoff: How Successful Businesses Build Customer Trust* (McGraw-Hill Ryerson, 2002)

CLO *Human Rights Call: A Summary of Twelve Instances of Human Rights Violations in Nigeria between January and October 1990*

Civil Liberties Organisation (CLO) *Human Rights Call: A Summary of Twelve Instances of Human Rights Violations in Nigeria between January and October 1990* (1990)

Clift "Data Protection and Data Exclusivity in Pharmaceuticals and Agrochemicals"

Clift C "Data Protection and Data Exclusivity in Pharmaceuticals and Agrochemicals" 431-433 in Krattiger A, Mahoney RT, Nelsen L, *et al* (eds) *Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best Practices* (MIHR, 2007)

Coetzee "Particularity in Morality and its Relation to Community"

Coetzee P H "Particularity in Morality and its Relation to Community" 275-317 in Coetzee P H and Roux A P J (eds.) *The African Philosophy Reader* (Routledge, 1998)

Cohen 1993 (22) Phil *&* *Pub Aff 207*

Cohen J "Freedom of Expression" *Philosophy and Public Affairs* Vol 22 No 3 (1993) 207-263

Cohen 2001 (89) *Geo L J 2029*

Cohen J E "Privacy, Ideology, and Technology: A Response to Jeffrey Rosen" *Georgetown Law Journal* Vol 89 (2001) 2029-2045

Cook *History of Political Philosophy from Plato to Burke*

Cook T I *History of Political Philosophy from Plato to Burke* (Pittman, 1936)

Cooley *A Treatise on the Law of Torts*

Cooley T *A Treatise on the Law of Torts* (Callaghan, 1888)

Colangelo 2007 (48) *Harv Int'l L J* 122

Colangelo A J "Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law" *Harvard International Law Journal* Vol 48 No 1 (2007) 122-201

Creech *Electronic Media Law and Regulation*

Creech C K *Electronic Media Law and Regulation* 3rd ed (Focal Press, 2000)

Culnan and Armstrong 1999 (10) No 1 *Organization Science* 104

Culnan M J and Armstrong P K "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation" *Organization Science* Vol 10 No 1 (1999) 104-115

Chang, Kaltani and Loayza 2009 (90) *J Dev Econ* 33

Chang R, Linda Kaltani and Norman V Loayza "Openness can be good for growth: The role of policy complementarities" *Journal of Development Economics* 2009 (90) 33–49

Chik 2006 (14) *IJLIT* 47

Chik W "The Lion, the Dragon and the Wardrobe: Guarding the Doorway to Information and Communications Privacy on the Internet: A Comparative Case Study of Hong Kong and Singapore – Two differing Asian Approaches" Vol 14 No 1 *International Journal of Law and Information Technology* (2006) 47–100

D

Damon 1986 (10) *Fordham Int'l L J* 262

Damon L J "Freedom of Information versus National Sovereignty: The Need for a New Global Forum for the Resolution of Transborder Data Flow Problems" *Fordham International Law Journal* Vol 10 No 2 (1986) 262-287

David "Structure and Divisions of the Law"

David R (Chief ed) *International Encyclopedia of Comparative Law* Vol II "The Legal Systems of the World, their Comparison and Unification" Chap 2: "Structure and Divisions of the Law" (1971)

Davies "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity"

Davies S G "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity" 143-165 in Agre P E and Rotenberg M (ed) *Technology and Privacy: The New Landscape* (MIT Press, 1997)

Davies March 2001 *UNESCO Courier* 18

Davies S "The Spy in Your Refrigerator" *UNESCO Courier* (March 2001) 18-19

Dempsey and Flint 2004 (72) *Geo Wash L Rev* 1459

Dempsey J X and Flint L M "Commercial Data and National Security" *George Washington Law Review* Vol 72 No 6 (2004) 1459-1502

De Roy 1997 (18) No 5 *TWQ* 883

De Roy O C "The African Challenge: Internet, Networking and Connectivity Activities in a Developing Environment" Vol 18 Issue 5 *Third World Quarterly* (1997) 883-898

Donnelly and Howard *International Handbook of Human Rights*

Donnelly J and Howard R E (eds) *International Handbook of Human Rights* (Greenwood, 1987)

Dutta and Mia *The Global Information Technology Report 2010–2011*

Dutta S and Mia I (eds) *The Global Information Technology Report 2010-2011* (World Economic Forum, Geneva 2011)

E

Edwards and Waeld (ed) *Law & The Internet: Regulating Cyberspace*

Edwards L and Waeld C (ed) *Law & The Internet: Regulating Cyberspace (*Hart Publishing 1997)

Ekpu *FOIA: Freedom for All*

Ekpu R "FOIA: Freedom For All" 9-12 in Arogundade L (ed) *FOIA (Freedom of Information Act) and Civil Society* (International Press Centre, 2003)

Eisenstein *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe*

Eisenstein E *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe* (Cambridge University Press 1980)

Elias *The Nature of African Customary Law*

Elias T O *The Nature of African Customary Law* (Manchester University Press, 1972)

EPIC and Privacy International *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*

EPIC and Privacy International *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (EPIC, 2006)

Eso *Thoughts on Law and Jurisprudence*

Eso K *Thoughts on Law and Jurisprudence* (M.I.J. Publications, Lagos 1991)

F

Fadipe *The Sociology of the Yoruba*

Fadipe N A *The Sociology of the Yoruba* (Ibadan University Press, 1970)

Fair 1987 (40) No 1 *ICG* 21

Fair J E "The Regulation of Transborder Data Flows: An International Law Perspective" *International Communication Gazette* Vol 40 No 1 (1987) 21-38

Farrell 2003 (57) *International Organisation* 277

Farrell H "Constructing the International Foundations of E-commerce: The EU-US Safe Harbor Arrangement" *International Organisation* Vol 57 No 2 (2003) 277–306

Feinberg *Social Philosophy*

Feinberg J *Social Philosophy* (Prentice-Hall, 1973)

Feketekuty *International Trade in Services: An Overview and Blueprint for Negotiations*

Feketekuty G International Trade in Services: An Overview and Blueprint for Negotiations (HarperCollins Canada, 1988)

Feldman 1983 (17) *TIL* 87

Feldman M "Commercial Speech, Transborder Data Flows and the Right to Communicate" *The International Lawyer* Vol 17 No1 (1983) 87-95

Feridun, Olusi and Folorunsho 2006 (6) *AIED* 174

Feridun M, Olusi J O and Folorunsho B A "Analysing the Impact of Globalization on Economic Development in Developing Economies: An Application of Error Correction Modelling (ECM) to Nigeria" *Applied Econometrics and International Development* Vol 6 No 3 (2006) 174-182

Flaherty *Privacy in Colonial New England*

Flaherty D *Privacy in Colonial New England* (University Press of Virginia, 1972)

Flaherty *Protecting Privacy in Surveillance Societies*

Flaherty D *Protecting Privacy in Surveillance Societies* (UNC Press, 1989)

Flaherty "Controlling Surveillance: Can Privacy Protection Be Made Effective"

Flaherty D "Controlling Surveillance: Can Privacy Protection Be Made Effective?" 167-192 in Agre P & Rotenberg M (eds) *Technology and Privacy: The New Landscape* (MIT Press, 1997)

Ford 2010 (2) *Wis L Rev* 441

Ford C "New Governance in the Teeth of Human Frailty: Lessons from Financial Regulation" *Wisconsin Law Review* Vol 2010 No 2 (2010) 441-487

Foord *Defining Privacy*

Foord K *Defining Privacy* (Victorian Law Reform Commission, 2002)

Froomkin 2000 (52) *Stan L Rev* 1464

Froomkin A M "The Death of Privacy?" 2000 (52) *Stanford Law Review* 1464-1543

Fried 1968 (77) *Yale L J* 475

Fried C "Privacy" *Yale Law Journal* Vol 77 No 3 (1968) 475-493

Fried "Privacy"

Fried C "Privacy" 203-222 in Schoeman F D (ed) *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press, 1984)

Fuchs 2001 (145) No 1 *Proc Am Phil Soc* 45

Fuchs I H "Prospects and Possibilities of the Digital Age" *Proceedings of the American Philosophical Society* Vol 145 No 1 (2001) 45-53

G

Gavison 1980 (89) *Yale L J* 421

Gavison R "Privacy and the Limits of Law" Vol 89 No 3 *Yale Law Journal* (1980) 421-471

Gellman "Does Privacy Law Work?"

Gellman R "Does Privacy Law Work?" 193-218 in Agre P and Rotenberg M (eds) *Technology and Privacy: The New Landscape* (MIT Press, 1997)

Gbadegesin *African Philosophy: Traditional Yoruba Philosophy and Contemporary African Realities*

Gbadegesin S *African Philosophy: Traditional Yoruba Philosophy and Contemporary African Realities* (Peter Lang, 1991)

Glancy 1979 (21) Ariz *L Rev* 1

Glancy D J "The Invention of the Right to Privacy" *Arizona Law Review* Vol 21 No 1 (1979) 1-39

Goldhill *Love, Sex, and Tragedy: How the Ancient World Shapes Our Lives*

Goldhill S *Love, Sex, and Tragedy: How the Ancient World Shapes Our Lives* (University of Chicago Press, 2005)

Gotlieb, Dalfen and Katz 1974 (68) *AJIL* 227

Gotlieb A, Dalfen C and Katz K "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles" *American Journal of International Law* 68 (1974) 227-257

Gow 2005 *Convergence* 76

Gow G A "Information Privacy and Mobile Phones" *Convergence* Vol 11 No 2 (2005) 76-87

Grabosky and Braithwaite *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies*

Grabosky P and Braithwaite J *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies* (Oxford University Press Inc., 1986)

Grewlich *Governance in 'Cyberspace': Access and Public Interest in Global Communications*

Grewlich *Governance in 'Cyberspace': Access and Public Interest in Global Communications* (Kluwer Law International, 1999)

Greenleaf 2012 (2) *IDPL* 68

Greenleaf G "The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108?" *International Data Privacy Law* Vol 2 No 2 (2012) 68-92

Greenleaf 2001 (4) *UNSWLJ* 262

Greenleaf G "Tabula Rasa – Ten Reasons Why Australian Privacy Law Does Not Exist" *University of New South Wales Law Journal* Vol 4 (2001) 262-269

Grove 1963 (7) *JAL* 152

Grove D L "The 'Sentinels' of Liberty? The Nigerian Judiciary and Fundamental Rights" *Journal of African Law* Vol 7 No 3 (1963) 152-171

Gunningham "**Beyond Compliance: Next Generation Environmental Regulation"**

Gunningham N "Beyond Compliance: Next Generation Environmental Regulation" 49-60 in Johnstone R and Sarre R (eds) *Regulation: Enforcement and Compliance* (Australian Institute of Criminology Research and Public Policy Series) No 57 (2004)

Guynes, Guynes and Thorn 1990 (6) No 3 *ISEJ* 27

Guynes J L, Guynes S C and Thorn R G "Conquering International Boundaries that Restrict the Flow of Data" *Information Strategy: The Executive's Journal* Vol 6 No 3 (1990) 27-32

Gyekye *The Unexamined Life: Philosophy and the African Experience*

Gyekye K *The Unexamined Life: Philosophy and the African Experience* (Ghana Universities Press, 1988)

H

Harter 2009 *J Disp Resol* 411

Harter P J "Collaboration: The Future of Governance" *Journal of Dispute Resolution* Vol 2009 No 2 (2009) 411-448

Hawkins *Environment and Enforcement: Regulation and the Social Definition of Pollution*

Hawkins K *Environment and Enforcement: Regulation and the Social Definition of Pollution* (Oxford University Press, Inc., 1984)

Held, McGrew, Goldblatt and Perraton J *Global Transformations: Politics, Economics and Culture*

Held D, McGrew A, Goldblatt D and Perraton J *Global Transformations: Politics, Economics and Culture* (Stanford University Press 1999)

Held and McGrew 1998 (24) *Rev Int'l Stud* 219

Held D and McGrew A "The End of the Old Order? Globalization and the Prospects for World Order" *Review of International Studies* Vol 24 No 5 (1998) 219-246

Heisenberg and Fandel *Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard*

Heisenberg D and Fandel M *Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard* 109-129 in Braman S (ed) *The Emergent Global Information Policy Regime* (Palgrave Macmillan, 2004)

Hirsch "Is Privacy Regulation the Environmental Law of the Information Age?"

Hirsch D D "Is Privacy Regulation the Environmental Law of the Information Age?" 239-253 in Strandburg K and Raicu D S (eds) *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* (Springer, 2006)

Hirschman *National Power and the Structure of Foreign Trade*

Hirschman A *National Power and the Structure of Foreign Trade* (University of California Press, 1980)

Hirst and Thompson 2002 (37) *Cooperation and Conflict* 247

Hirst P and Thompson G "The Future of Globalization" *Cooperation and Conflict: Journal of the Nordic International Studies Association* Vol 37 No 3 (2002) 247-265

Hobbes *Leviathan*

Hobbes T *Leviathan* (Digireads.com Publishing, 2009)

Hofstede *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*

Hofstede G *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations* 2nd ed (SAGE Publications Inc., 2001)

Hofstede *Cultures and Organisations: Intercultural Cooperation and its Importance for Survival*

Hofstede G *Cultures and Organisations: Intercultural Cooperation and its Importance for Survival* (HarperCollins, 1994)

Hofstede *Culture's Consequences: International Differences in Work-Related Values*

Hofstede G *Culture's Consequences: International Differences in Work-Related Values* (SAGE, 1980)

Hofstede *Cultures and Organizations: Software of the Mind*

Hofstede G *Cultures and Organizations: Software of the Mind* (McGraw-Hill, 1997)

Hornung and Schnabel 2009 (25) *C L S Rev* 84

Hornung G and Schnabel C "Data protection in Germany I: The population census decision and the right to informational self-determination" *Computer Law & Security Review* Vol 25 No 1 (2009) 84-88

Howard "Group versus Individual Identity in the African Debate on Human Rights"

Howard R "Group versus Individual Identity in the African Debate on Human Rights" 155-179 in An-Naim A A and Deng F M (eds) *Human Rights in Africa: Cross-Cultural Perspectives* (Brookings Institution Press, 1990)

Howard *Human Rights in Commonwealth Africa*

Howard R E *Human Rights in Commonwealth Africa* (Rowman & Littlefield, 1986)

Howard and Donnelly 1986 (80) *Am Polit Sci Rev* 801

Howard R E and Donnelly J "Human Dignity, Human Rights and Political Regimes" *American Political Science Review* Vol 80 No 3 (1986) 801-817

Hoyle 1992 (8) No 4 *C L S Rev* 166

Hoyle C "Legal Aspects of Trans-border Data Flow" *Computer Law and Security Report* Vol 8 No 4 (1992) 166-172

Huskey and Velma 1976 (C-25) No 12 *IEEE Transactions on Computers* 1190

Huskey H D & Velma R "Chronology of Computing Devices" *IEEE Transactions on Computers* Vol C-25 No 12 (1976) 1190-1199

Hutter *Compliance: Regulation and Environment*

Hutter B M *Compliance: Regulation and Environment* (Clarendon Press, 1997)

J

Jayasuriya 1999 (6) No 2 *Ind J Global Legal Stud* 425

Jayasuriya K "Globalisation, Law and the Transformation of Sovereignty: The Emergence of Global Regulatory Governance" *Indiana Journal of Global Legal Studies* Vol 6 No 2 (1999) 425 -455

Joseph *Democracy and Prebendal Politics in Nigeria: The Rise and fall of the Second Republic*

Joseph R A *Democracy and Prebendal Politics in Nigeria: The Rise and fall of the Second Republic* (Spectrum Books, 1987)

Jussawalla *Information Economies and the Development of Pacific Countries*

Jussawalla M "Information Economies and the Development of Pacific Countries" 15-24 in Jussawalla M Dervin B, Lamberton D and Karunaratne N (eds) *The Cost of Thinking: Information Economies of Ten Pacific Countries* (Greenwood Publishing Group 1988)

Jussawalla and Cheah 1983 (7) *Telecommunications Policy* 285

Jussawalla M and Cheah C "Emerging Economic Constraints on Transborder Data Flows" *Telecommunications Policy* Vol 7 No 4 (1983) 285-296

K

Kang 1998 (50) *Stan L Rev* 1193

Kang J "Information Privacy in Cyberspace Transactions" Vol 50 No 4 *Stanford Law Review* (1998) 1193-1294

Kaiser 2010 (6) No 3 *EuConst* 503

Kaiser A-B "German Federal Constitutional Court: German Data Retention Provisions Unconstitutional in Their Present Form; Decision of 2 March 2010, NJW 2010, 833." *European Constitutional Law Review* Vol 6 No 3 (2010) 503-517

Keohane and Nye *Power and Interdependence*

Keohane R O and Nye J *Power and Interdependence* (Longman, 1989)

Kirkman et al *The Global Information Technology Report 2001-2002*

Kirkman G, Cornelius P K, Sachs J D and Schwab K *The Global Information Technology Report 2001-2002* (Oxford University Press, USA, 2002))

Kling and Allen "How the Marriage of Management and Computing Intensifies the Struggle for Personal Privacy"

Kling R and Allen J P "How the Marriage of Management and Computing Intensifies the Struggle for Personal Privacy" 104-131 in Lyon D & Zureik E (eds) *Computers, Surveillance, and Privacy* (University of Minnesota Press, 1996)

Knoppers 1984 (9) *J Technology Transfer* 1

Knoppers J V T "Transborder Data Flow Issues and Technology Transfer" *Journal of Technology Transfer* Vol 9 No 1 (1984) 1-14

Kobrin "Globalization, Transnational Corporations and the Future of Global Governance"

Kobrin S J "Globalization, Transnational Corporations and the Future of Global Governance*"* 249-272 in Scherer A G and Palazzo G (eds) *Handbook of Research on Global Corporate Citizenship* (Cheltenham, UK, and Northampton, MA: Edward Elgar, 2008)

Kobrin 2004 (30) *Rev Int'l Stud* 111

Kobrin S J "Safe Harbours are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance" *Review of International Studies* Vol 30 No 1 (2004) 111-131

Kobrin No 107 *Foreign Policy* (1997) 65

Kobrin S J "Electronic Cash and the End of National Markets" *Foreign Policy* No 107 (1997) 65-77

Kobrin 2001 (32) *J Int Bus Stud* 687

Kobrin S J "Territoriality and the Governance of Cyberspace" *Journal of International Business Studies* Vol 32 No 4 (2001) 687-704

Kranzberg "The Information Age: Evolution or Revolution?"

Kranzberg M "The Information Age: Evolution or Revolution?" 35-53 in Guile B (ed) *Information Technologies and Social Transformation* (1985)

Krasner 2001 (22) *IPSR* 229

Krasner S D "Abiding Sovereignty" *International Political Science Review* Vol 22 No 3 (2001) 229-251

Kuner 2009 (25) *C L S Rev* 307

Kuner C "An International Legal Framework for Data Protection: Issues and Prospects" *Computer Law & Security Review* Vol 25 No 4 (2009) 307-317

Kusamotu 2007 (16) *Info & Comm Tech L* 149

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* Vol 16 No 2 (2007) 149-159

L

Lassiter 2000 (3) *ASQ*

Lassiter J E "African Culture And Personality: Bad Social Science, Effective Social Activism, Or A Call To Reinvent Ethnology?" *African Studies Quarterly* Vol 3 No 3 (2000)

Leary *The Effect of Western Perspectives on International Human Rights*

Leary V A "The Effect of Western Perspectives on International Human Rights" 15-26 in An-Naim A A and Deng F M (eds) *Human Rights in Africa: Cross-Cultural Perspectives* (Brookings Institution Press, 1990)

Leenes and Koops 2005 (12) *Mich Telecomm & Tech L Rev* 115

Leenes R and Koops B-J "Code' and Privacy or How Technology is Slowly Eroding Privacy" Vol 12 No 1 *Michigan Telecommunications & Technology Law Review* (2005) 115-188

Lessig 1996 (45) *Emory L J* 1

Lessig L "Reading the Constitution in Cyberspace" 45 *Emory Law Journal* (1996) 1-44

Lewis P *Growing Apart: Oil, Politics, and Economic Change in Indonesia and Nigeria*

Lewis P *Growing Apart: Oil, Politics, and Economic Change in Indonesia and Nigeria* (University of Michigan Press, 2007)

Lipton 2001 (6) *J Tech L & Pol'y* 1

Lipton J "Protecting Valuable Commercial Information in the Digital Age" *Journal of Technology Law & Policy* Vol 6 No 1 (2001) 1-30

Liu *Extraterritoriality: Its Rise and Its Decline*

Liu S S *Extraterritoriality: Its Rise and Its Decline* (Columbia University, 1925)

Locke *The Second Treatise of Government*

Locke J *The Second Treatise of Government* (C. Baldwin, 1824)

Lowry 1984 (6) *Hous J Int'l L* 159

Lowry H P "Transborder Data Flow: Public and Private International Law Aspects" *Houston Journal of Internatioinal Law* Vol 6 No 159 (1984) 159-174

Lucien and Martin *The Coming of the Book: The Impact of Printing 1450-1800*

Lucien F and H J Martin *The Coming of the Book: The Impact of Printing 1450-1800* (Verso Classics 1976)

M

MacBride Commission *Many Voices, One World: Towards a New, More Just, and More Efficient World Information and Communication Order*

MacBride Commission *Many Voices, One World: Towards a New, More Just, and More Efficient World Information and Communication Order* (Rowman & Littlefield Publishing Group, 2004)

Machlup *The Production and Distribution of Knowledge in the United States*

Machlup F *The Production and Distribution of Knowledge in the United States* (Princeton University Press 1962)

Maherzi) *World Communication Report: The Media and the Challenge of the New Technologies*

Maherzi L *World Communication Report: The Media and the Challenge of the New Technologies* (UNESCO Publishing Paris, 1997)

Mahmoud 1993 (15) *Hum Rts Q* 485

Mahmoud S S "The State and Human Rights in Africa in the 1990s: Perspectives and Prospects" *Human Rights Quarterly* Vol 15 No 3 (1993) 485-498

Majone 1994 (17) *W Eur Pol* 77

Majone G "The Rise of the Regulatory State in Europe" *West European Politics* Vol 17 No 3 (1994) 77-101

Mansell and Wehn *Knowledge Societies: Information Technology for Sustainable Development*

Mansell R and Wehn U *Knowledge Societies: Information Technology for Sustainable Development* (United Nations Publications 1998)

Markus and Kitayama 1991 (98) *Psychological Review* 224

Markus and Kitayama "Culture and Self: Implications for Cognition, Emotion and Motivation" *Psychological Review* Vol 98 No 2 (1991) 224-253

Marsden 2001 (2) *Det C L Mich St U L Rev* 355

Marsden C T "Cyberlaw and International Political Economy: Towards Regulation of the Global Information Society" *Detroit College of Law at Michigan State University Law Review* Law Vol 2 (2001) 355-422

Mattli and Buthe 2003 (56) *World Politics* (2003) 1

Mattli W and Buthe T "Setting International Standards: Technological Rationality or Primacy of Power?" *World Politics* Vol 56 No 1 (2003) 1-42

Martyn 1986 (12) 4 *IFLA Journal* 318

Martyn J "Transborder Data Flow: An Introduction" *International Federation of Library Associations and Institutions Journal* Vol 12 No 4 (1986) 318-321

Mason "The Relationship Between Freedom of Expression and Freedom of Information"

Mason A "The Relationship Between Freedom of Expression and Freedom of Information" 225-238 in Beatson J and Cripps Y (eds) *Freedom of Expression and Freedom of Information: Essays in Honour of Sir David Williams* (Oxford University Press, 2000)

Mbiti *African Religions and Philosophy*

Mbiti J S *African Religions and Philosophy* (Heinemann, 1969)

Mbiti *Introduction to African Religion*

Mbiti J S *Introduction to African Religion* 2nd ed (Heinemann, 1991)

McCamus 1986 (3) *Gov Inf Q* 49

McCamus J D "The Delicate Balance: Reconciling Privacy Protection with the Freedom of Information Principle" *Government Information Quarterly* Vol 3 No 1 (1986) 49-61

McAnany *Communications in the Rural Third World: The Role of Information in Development:* The Role of Information in Development

McAnany E G (Ed) *Communications in the Rural Third World: The Role of Information in Development* (Praeger, 1980)

Mckeon 1994 (7) *J Marshall J Computer & Info L* 511

Mckeon Jr. R W "Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena" Vol 7 No 4 *John Marshall Journal of Computer and Information Law* (1994) 511-536

Mellors and Pollitt 1984 (37) *Parliamentary Affairs* 199

Mellors C and Pollitt D "Legislating for Privacy: Data Protection in Western Europe*"* *Parliamentary Affairs* Vol 37 No 2 (1984) 199-215

Mendel *Freedom of Information: A Comparative Legal Survey*

Mendel T *Freedom of Information: A Comparative Legal Survey* (UNESCO, 2003)

Mendel 2003 (1) *Comparative Media Law Journal*

Mendel T "Freedom of Information as an Internationally Protected Human Right" *Comparative Media Law Journal* (online journal) No 1 (2003). Available at: <http://www.juridicas.unam.mx/publica/rev/comlawj/cont/1/cts/cts3.htm>. [Accessed 8/5/13]

Messick 1999 (14) *WBRO* 1

Messick R E "Judicial Reform and Economic Development: A Survey of the Issues" *The World Bank Research Observer* Vol 14 No 1 (1999) 1-8

Mhlaba 1995 (12) *GIQ* 353

Mhlaba S L "The Efficacy of International Regulation of Transborder Data Flows: The Case for the Clipper Chip" *Government Information Quarterly* Vol 12 No 4 (1995) 353-366

Michael 1995 (47) *Admin L Rev* 171

Michael D C "Federal Agency Use of Audited Self-Regulation as a Regulatory Technique" *Administrative Law Review* Vol 47 No 2 (1995) 171-254

Michael *Privacy and Human Rights*

Michael J *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (UNESCO Publishing, 1994)

Miller 1996 (1) *Communications Law* 143

Miller T "Law, Privacy and Cyberspace" *Communications Law* Vol 1 No 4 (1996) 143-148

Miller *The Assault on Privacy*

Miller A *The Assault on Privacy* (Univ. of Mich. Press, 1971)

Mills *Principles of Political Economy*

Mills J S *Principles of Political Economy with some of their applications to Social Philosophy*, Nathanson S (ed) (Hackett Publishing Company Inc., 2004)

Milberg, Smith and Burke 2000 (11) No 1 *Organization Science* 35

Milberg S J, Smith H J and Burke S J "Information Privacy: Corporate Management and National Regulation" *Organization Science* Vol 11 No 1 (2000) 35-57

Milberg, Burke, Smith and Kallman 1995 (38) *Commun ACM* 65

Milberg S J, Burke S J, Smith H J and Kallman E A "Values, Personal Information, Privacy, and Regulatory Approaches" *Communications of the ACM* Vol 38 No 12 (1995) 65-74

Minogue and Carino *Regulatory Governance in Developing Countries*

Minogue M and Carino L V *Regulatory Governance in Developing Countries* (Edward Elgar Publishing, 2007)

Ministry of Communications, Nigeria *National Policy on Telecommunications* (2000)

Ministry of Commerce, Nigeria *Trade Policy of Nigeria* (2001)

Moemeka 1998 (48) *Journal of Communication* 118

Moemeka A "Communalism as a Fundamental Dimension of Culture" *Journal of Communication* Vol 48 No 4 (1998) 118–141

Mojekwu *International Human Rights: The African Perspective*

Mojekwu C "International Human Rights: The African Perspective" in Nelson J L and Green V (eds) *International Human Rights: Contemporary Issues* (Human Rights Publishing Group, 1980)

Moore 1965 (38) No 8 *Electronics* 114

Moore G "Cramming more components onto integrated circuits" Vol 38 No 8 *Electronics* 114 - 117. (Reprinted in *Solid State Circuits Newsletter, IEEE* Vol 11 No 5 33)

Moor "Towards a Theory of Privacy for the Information Age"

Moor J "Toward a Theory of Privacy for the Information Age" 407-417 in Spinello R and Tavani H (eds) *Readings in CyberEthics* (Jones & Bartlett Learning, 2004)

Moore *Privacy: Studies in Social and Cultural History*

Moore B *Privacy: Studies in Social and Cultural History* (M.E. Sharpe, 1984)

Morgan 2003 (62) *C L J* 444

Morgan A "Privacy, Confidence and Horizontal Effect: "Hello" Trouble" *Cambridge Law Journal* Vol 62 No 2 (2003) 444 -473

Morriss, Yandle and Dorchak 2005 (29) *Harv Envtl L Rev* 179

Morriss A P, Yandle B and Dorchak A "Choosing How to Regulate" *Harvard Environmental Law Review* Vol 29 No 1 (2005) 179-250

Mowlana *Global Information and World Communication*

Mowlana H *Global Information and World Communication* 2nd ed (Sage Publications 1997)

Mowlana *International Flow of Information: A Global Report and Analysis*

Mowlana H *International Flow of Information: A Global Report and Analysis* (UNESCO 1985)

Movius and Krup 2009 (3) *IJC* 169

Movius L B and Krup N "US and EU Privacy Policy: Comparison of Regulatory Approaches" Vol 3 *International Journal of Communication* (2009) 169-187

Mkandawire and Soludo *African Voices on Structural Adjustment: A Companion to Our Continent, Our Future*

Mkandawire T & Soludo C C (ed) *African Voices on Structural Adjustment: A Companion to Our Continent, Our Future* (IDRC, 2003)

Murray *The Regulation of Cyberspace: Control in the Online Environment*

Murray A *The Regulation of Cyberspace: Control in the Online Environment* (Routledge, 2007)

N

National Research Council *The Digital Dilemma: Intellectual Property in the Information Age*

National Research Council (USA), Committee on Intellectual Property Rights in the Emerging Information Infrastructure *The Digital Dilemma: Intellectual Property in the Information Age* (National Academy Press 2000)

Neethling, Potgieter and Visser *Neethling's Law of Personality*

Neethling J, Potgieter J M and Visser P J *Neethling's Law of Personality* (Lexis Nexis, South Africa, 2005)

Neogi and Cordell 2010 (15) No 2 *JIB&C* 1

Neogi P K & Cordell A J "The Internet and the Need for Governance: Learning from the Past, Coping with the Future" *Journal of Internet Banking and Commerce* Vol 15 No 2 (2010) 1-30

Nimmer and Krauthaus 1992 (55) Law *& Contemp Probs* 103

Nimmer R T and Krauthaus P A "Information as a Commodity: New Imperatives of Commercial Law" *Law and Contemporary Problems* 1992 Vol 55 No 3 (1992)103 – 130

Novotny 1980 (16) No 1 *Stan J Int'l L* 141

Novotny E J "Trans-border Data Flow and International Law: A Framework for Policy-Oriented Inquiry" *Stanford Journal of International Law Vol* 16 No 1 (1980) 141-157

Nugter *Transborder Flow within the EEC*

Nugter A *Transborder Flow within the EEC* (Springer, 1990)

Nwadialo *Modern Nigerian Law of Evidence*

Nwadialo F *Modern Nigerian Law of Evidence* (Ethiope Publishing Corporation, 1981)

Nwabueze "Role of Judiciary in the Conflict between Freedom of the Individual and the State Power"

Nwabueze B "*Role of Judiciary in the Conflict between Freedom of the Individual and the State Power"* in *The Guardian* newspaper (5th Sept. 2006) at 69

Nwabueze *Presidentialism in Commonwealth Africa*

Nwabueze B O *Presidentialism in Commonwealth Africa* (St. Martin's Press, 1974)

Nwabueze Military *Rule and Constitutionalism*

Nwabueze B 0 Military *Rule and Constitutionalism* (Spectrum Law Publishing, 1992)

Nyasani *The African Psyche*

Nyasani J M *The African Psyche* (J.M. Nyasani, 1997)

O

Obe *The Challenging Case of Nigeria*

Obe A "The Challenging Case of Nigeria" in Florini A (ed) *The Right To Know: Transparency for an Open World* (Columbia University Press, 2007)

Obilade *The Nigerian Legal System*

Obilade A O *The Nigerian Legal System* (Sweet & Maxwell, 1979)

Ogowewo 1995 (39) *JAL* 1

Ogowewo T I "The Problem with Standing to Sue in Nigeria" *Journal of African Law* Vol. 39 No 1 (1995) 1-18

Ogundiya 2009 (11) *Anthropologist* 281

Ogundiya I S "Political Corruption in Nigeria: Theoretical Perspectives and Some Explanations" *Anthropologist* Vol 11 No 4 (2009) 281-292

O'Harrow *No Place to Hide*

O'Harrow R Jr *No Place to Hide* (Free Press, 2005)

Ohmae *The End of the Nation State: The Rise of Regional Economies*

Ohmae K *The End of the Nation State: The Rise of Regional Economies* (Free Press Paperbacks 1996)

Okigbo *Essays in the Public Philosophy of Development Vol 3: Growth and Structure of the Nigeria Economy*

Okigbo P *Essays in the Public Philosophy of Development Vol 3: Growth and Structure of the Nigeria Economy* (Fourth Dimension Publishing Company, 1993)

Okpaku (ed) *Information and Communication Technologies for African Development: An Assessment of Progress and the Challenges Ahead*

Okpaku J O (ed) *Information and Communication Technologies for African Development: An Assessment of Progress and the Challenges Ahead* (United Nations Publications, 2003)

Olusanya 1970 (32) *J Marriage & Fam* 150

Olusanya P O "Notes on Some Factors Affecting the Stability of Marriage among the Yoruba of Western Nigeria" *Journal of Marriage and the Family* Vol 32 (1970) 150-155

Oyejide, Ogunkola and Bankole "Quantifying the Trade Impact of Sanitary and Phytosanitary Standards: What is Known and Issues of Importance for Sub-Saharan Africa"

Oyejide T A, Ogunkola O and Bankole A "Quantifying the Trade Impact of Sanitary and Phytosanitary Standards: What is Known and Issues of Importance for Sub-Saharan Africa" 185-218 in Maskus K E and Wilson J S (eds.) *Quantifying the Trade Effect of Technical Barriers: Can it be Done?* (2001)

P

Palmer "Freedom of Information: The New Proposals"

Palmer S "Freedom of Information: The New Proposals" 249-266 in Beatson J and Cripps Y (eds) *Freedom of Expression and Freedom of Information: Essays in Honour of Sir David Williams* (Oxford University Press, 2000)

Paterson 1998 (26) *Fed L Rev* 371

Paterson M "Privacy Protection in Australia: The Need for an Effective Private Sector Regime" *Federal Law Review* Vol 26 No 2 (1998) 371-400

Paul "Participatory Approaches to Human Rights in Sub-Saharan Africa"

Paul J C N "Participatory Approaches to Human Rights in Sub-Saharan Africa" 209-236 in An-Naim A A and Deng F M (eds) *Human Rights in Africa: Cross-Cultural Perspectives* (1990)

Peltzman 1976 (19) *J L & Econ* 211

Peltzman S "Toward a More General Theory of Regulation" *Journal of Law and Economics* Vol 19 No 2 (1976) 211-240

Perelman 1996 (2) *Mich Telecomm & Tech L Rev* 93

Perelman M "Software Patents and the Information Economy" *Michigan Telecommunications and Technology Law Review* Vol 2 (1996) 93-102

Perez-Albuerne and Friedman 2001 (19) No 3 *J Marshall J Computer & Info L* 435

Perez-Albuerne C and Friedman L "Privacy Protection for Electronic Communications and the "Interception Unauthorized Access" Dilemma" *John Marshall Journal of Computer & Information Law* Vol 19 No3 (2001) 435-456

Pipe 1985 (1) No 4 *Telematics and Informatics* 409

Pipe R "International Information Policy: Evolution of Transborder Data Flow Issues" *Telematics and Informatics* Vol 1 No 4 (1985) 409-418

Pollis "Liberal, Socialist, and Third World Perspectives of Human Rights"

Pollis A "Liberal, Socialist, and Third World Perspectives of Human Rights" 1-26 in Schwab P and Pollis A *Toward a Human Rights Framework* (Praeger, 1982)

Porat *The Information Economy: Definition and Measurement*

Porat M U *The Information Economy: Definition and Measurement* Vol 1-8 (Dept. of Commerce, Office of Telecommunications, 1977)

Posner 1978 (12) *Ga L Rev* 393

Posner R "The Right to Privacy" *Georgia Law Review* Vol 12 **(**1978) 393-422

Posner 1998 (13) *World Bank Res Obs* 1

Posner R "Creating a Legal Framework for Economic Development" *The World Bank Research Observer* Vol 13 no 1 (1998) 1-11

Posner 1974 (5) *Bell J Econ Manag Sci* 335

Posner R A "Theories of Economic Regulation" *Bell Journal of Economics and Management Science* Vol 5 No 2 (1974) 335-358

Post 1989 (77) No 5 *Cal L Rev* 957

Post R C "The Social Foundations of Privacy: Community and Self in the Common Law Tort" *California Law Review* Vol 77 No 5 (1989) 957-1010

Post and Johnson 1996 (48) *Stan L Rev* 1367

Post D and Johnson D "Law and Borders - The Rise of Law in Cyberspace" *Stanford Law Review* Vol 48 (1996) 1367-1402

Poullet 2007 (2) *JICLT* (2007) 141

Poullet Y "Transborder Data Flows and Extraterritoriality: The European Position" *Journal of International Commercial Law and Technology* Vol 2 No 3 (2007) 141-153

Poullet Directive 2002/58/EC

Poullet Y "Directive 2002/58/EC" 145-204 in Bullesbach A, Poullet Y and Priens C (eds) *Concise European IT Law* (Kluwer Law International, 2006)

Prosser 1960 (48) *Cal L Rev* 383

Prosser W L "Privacy" *California Law Review* Vol 48 No 3 (1960) 383-423

Q

Qiang, Clarke and Halewood "The Role of ICT in Doing Business"

Qiang C Z-W, Clarke G R, and Halewood N "The Role of ICT in Doing Business" in *World Bank Report: Information and Communications for Development: Global Trends and Policies* (The World Bank, 2006)

R

Rajaee *Globalisation on Trial: The Human Condition and Information Civilization*

Rajaee F *Globalisation on Trial: The Human Condition and Information Civilization* (International Development Research Centre, 2000)

Ramage *Privacy: Law of Civil Liberties*

Ramage S *Privacy: Law of Civil Liberties* (iUniverse, 2007)

Regan *Legislating Privacy*

Regan P M *Legislating Privacy* (Univ of North Carolina Press, 1995)

Regan 1993 (52) *Am J Econ Sociol* 257

Regan P M "The Globalisation of Privacy: Implications of Recent Changes in Europe" *American Journal of Economics and Sociology* Vol 52 No 3 (1993) 257-274

Regan 2003 (59) No 2 *J Soc Issues* 263

Regan P "Safe Habors or Free Frontiers? Privacy and Trans-border Data Flows" *Journal of Social Issues* Vol 59 No 2 (2003) 263-282

Reidenberg 2001 (38) *Hous L Rev* 717

Reidenberg J R "E-commerce and Trans-Atlantic Privacy" 2001 (38) *Houston Law Review* 717-749

Reidenberg 1992 (44) No 2 *Fed Comm L J* 195

Reidenberg J R "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" *Federal Communications Law Journal* Vol 44 No 2 (1992) 195-243

Reidenberg 2000 (52) No 5 *Stan L Rev* 1315

Reidenberg J R "Resolving Conflicting International Data Privacy Rules in Cyberspace" *Stanford Law Review* Vol 52 No 5 (2000) 1315-1376

Reidenberg 1992 (60) No 6 *Fordham L Rev* 137

Reidenberg J R "The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services" *Fordham Law Review* Vol 60 No 6 (1992) 137-177

Reidenberg 1993 (6) *Harv J L & Tech* 287

Reidenberg J R "Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms" Vol 6 No 2 *Harvard Journal of Law & Technology* (1993) 287-305

Roberts 2001 (51) *U T L J* 243

Roberts A "Structural Pluralism and the Right to Information" *University of Toronto Law Journal* Vol 51 No 3 (2001) 243-271

Roberts and Gregor *Privacy: A Cultural View*

Roberts J M and Gregor T "Privacy: A Cultural View" 199-225 in Pennock J R and Chapman J W (eds) *Privacy: Nomos XIII* (Atherton, 1971)

Robinson 1983 (7) *Telecommunications Policy* 267

Robinson P "TDF: The Hardy Perennial" *Telecommunications Policy* Vol 7 Issue 4 (1983) 267-344

Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study*

Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD Thesis UNISA, 2003)

Rosen *The Unwanted Gaze: The Destruction of Privacy in America*

Rosen J *The Unwanted Gaze: The Destruction of Privacy in America* (Knopf Doubleday Publishing Group, 2000)

Rosenau *Turbulence in World Politics: A Theory of Change and Continuity*

Rosenau J *Turbulence in World Politics: A Theory of Change and Continuity* (Princeton University Press, 1990)

Rosenberg *A Background Review of the Relationships Between Technological Innovation and the Economy*

Rosenberg N "A Background Review of the Relationships Between Technological Innovation and the Economy" 18-48 in Katz M, Graham E M and Schwartz J *Technology, Trade and the U.S. Economy* (National Academy of Sciences, 1978)

Rotenberg 2001 (1) *Stan Tech L Rev* 1

Rotenberg M "Fair Information Practices and the Architecture of Privacy: What Larry Doesn't Get" 2001 (1) *Stanford Technology Law Review* 1-4

Rothfeder *Privacy for Sale*: *How Computerization Has Made Everyone's Private Life an Open Secret*

Rothfeder J *Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret* (Simon & Schuster 1992)

Rubinstein, Ronald and Schwartz 2008 (75) *U Chi L Rev* 261

Rubinstein I S, Ronald D L and Schwartz P M "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches" *University of Chicago Law Review* Vol 75 No 1 (2008) 261-285

S

Salacuse 1999 (33) *Int Lawyer* 875

Salacuse J W "From Developing Countries to Emerging Markets: A Changing Role for Law in the Third World" *The International Lawyer* Vol 33 No 4 (1999) 875 – 890

Salbu 2002 (35) *Vand J Transnat'l L* 655

Salbu S R "The European Union Data Privacy Directive and International Relations" *Vanderbilt Journal of Transnational Law* Vol 35 No 2 (2002) 655-696

Samuelson 2000 (52) *Stan L Rev* 1125

Samuelson P "Privacy as Intellectual Property?" 2000 (52) *Stanford Law Review* 1125-1173

Samiee 1984 (15) *J Int Bus Stud* 141

Samiee S "Transnational Data Flow Constraints: A New Challenge for Multinational Corporations" *Journal of International Business Studies* Vol 15 No 1 (1984) 141–150

Sauvant 1983 (37) *International Organisation* 359

Sauvant K P "Transborder Data Flows and the Developing Countries" *International Organisation* Vol 37 No 2 (Spring 1983) 359-371

Savage and Edwards 1986 (35) *Int'l & Comp L Q* 710

Savage N and Edwards C "Transborder Data Flows: The European Convention and the United Kingdom Legislation" *International and Comparative Law Quarterly* Vol 35 No 3 (1986) 710-717

Scarpa *The Theory of Quality Regulation and Self-Regulation*

Scarpa C "The Theory of Quality Regulation and Self-Regulation" in Bortolotti B and Fiorentini G (eds) *Organised Interests and Self-Regulation: An Economic Approach* (Oxford University Press, 1999)

Schware *Overview: E-Development: From Excitement to Effectiveness*

Schware R "Overview: E-Development: From Excitement to Effectiveness" xiii-xxii in Schware R (ed) *E-Development: From Excitement to Effectiveness* (World Bank Publications, 2005)

Schwartz 1999 (52) *Vand L Rev* 1609

Schwartz P M "Privacy and Democracy in Cyberspace" *Vanderbilt Law Review* Vol 52 (1999) 1609-1702

Schwartz and Reidenberg *Data Privacy Law: A Study of United States Data Protection*

Schwartz P and Reidenberg J *Data Privacy Law: A Study of United States Data Protection* (Lexis Law Pub, 1996)

Seidman 1966 *Wis L Rev* 999

Seidman R "Law and Economic Development in Independent, English-speaking Sub-Saharan Africa" *Wisconsin Law Review* (1966) 999-1070

Senn *Non-state Regulatory Responses: Understanding Institutional Transformation*

Senn M *Non-state Regulatory Responses: Understanding Institutional Transformation* (Walter De Gruyter Incorporated, 2010)

Shaffer 2000 (25) *Yale J Int'l L* 1

Shaffer G C "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Data Privacy Standards" Vol 25 *Yale Journal of International Law* (2000) 1-88

Shapiro and Varian *Information Rules: A Strategic Guide to the Network Economy*

Shapiro C and Varian H R *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Press, 1999)

Shaw M *International Law*

Shaw M *International Law* 6th ed (Cambridge University Press, 2008)

Sieghart *Privacy and Computers*

Sieghart P *Privacy and Computers* (Latimer London, 1976)

Solove 2006 (154) No 3 *U Pa L Rev* 477

Solove D J "A Taxonomy of Privacy" *University of Pennsylvania Law Review* Vol 154 No 3 (2006) 477-560

Solove 2002 *Cal L Rev* 1087

Solove D J "Conceptualizing Privacy" *California Law Review* Vol 90 (2002) 1087-1156

Solove *The Digital Person*

Solove D J *The Digital Person: Technology and Privacy in the lnformation Age* (NYU Press, 2004)

Solove *Understanding Privacy*

Solove D J *Understanding Privacy* (Harvard University Press, 2008)

Solove and Rotenberg *Information Privacy Law*

Solove D J and Rotenberg M *Information Privacy Law* (Aspen Publishers, 2003)

Solove and Hoofnagle 2006 No 2 *U Ill L Rev* 357

Solove D J & Hoofnagle C J "A Model Regime of Privacy Protection" *University of Illinois Law Review* Vol 2006 No 2 (2006) 357-404

Sorenson 1998 (24) *Rev Int'l Stud* 83

Sorenson G "IR Theory after the Cold War" *Review of International Studies* Vol 24 No 5 (1998) 83-100

Soubbotina and Sheram *Beyond Economic growth: Meeting the Challenges of Global Development*

Soubbotina T P and Sheram K A *Beyond Economic growth: Meeting the Challenges of Global Development* (The World Bank, Washington 2000)

Spinello 2011 (16) No 12 *IRIE* 41

Spinello R A "Privacy and Social Networking Technology" *International Review of Information Ethics* Vol 16 No 12 (2011) 41-46

Stahl 1994 (19) *Yale J Int'l L* 405

Stahl T H "Liberalising International Trade in Service: The Case of Side-stepping GATT" Vol 19 *Yale Journal of International Law* (1994) 405-454

Stigler 1971 (2) *Bell J Econ Manag Sci* 3

Stigler G "The Theory of Economic Regulation" *Bell Journal of Economics and Management Science* Vol 2 No 1 (1971) 3-21

Stover *Information Technology in the Third World: Can IT Lead to Humane National Development?*

Stover W J *Information Technology in the Third World: Can IT Lead to Humane National Development?* (Westview Press, 1984)

Strange *The Retreat of the State: The Diffusion of Power in The World Economy*

Strange S *The Retreat of the State: The Diffusion of Power in The World Economy* (Cambridge University Press, 1996)

Strauss and Rogerson 2002 (19) *Telematics and Informatics* 173

Strauss J and Rogerson K S "Policies for Online Privacy in the United States and the European Union" *Telematics and Informatics* Vol 19 No 2 (2002) 173–192

Stuntz 1995 (93) *Mich L Rev* 1016

Stuntz W J "Privacy's Problem and the Law of Criminal Procedure" 1995 (93) *Michigan Law Review* 1016-1078

Sullivan 1992 (106) *Harv L Rev* 22

Sullivan K M "The Justices of Rules and Standards" *Harvard Law Review* Vol 106 No 22 (1992) 22-123

Swire and Litan *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*

Swire P and Litan R E *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings Institution Press, 1998)

T

Tavani 2005 (3) No 6 *IRIE* 39

Tavani H T "Search Engines, Personal Information and the Problem of Privacy in Public" *International Review of Information Ethics* Vol 3 No 6 (2005) 39-45

Tavani and Moor 2001 (31) No 1 *Computers and Society* 6

Tavani H & Moor J "Privacy Protection, Control of Information and Privacy-Enhancing Technologies" *Computers and Society* Vol 31 No 1 (2001) 6-11

Taylor 2000 (26) *Monash U L Rev* 235

Taylor G "Why is there no Common Law Right of Privacy?" Vol 26 No 2 *Monash University Law Review* (2000) 235-274

Teece 2010 (43) *LRP* 172

Teece D J "Business Models, Business Strategy and Innovation" *Long Range Planning* Vol 43 (2010) 172-194

Todaro and Smith *Economic Development*

Todaro M P and Smith S C *Economic Development* (8th ed) (Addison Wesley, 2003)

***The World Book Encyclopaedia* Vol 19 (World Book, Inc, Chicago, 2002)**

***The World Book Encyclopaedia* Vol 15 (World Book, Inc, Chicago, 2002)**

***The World Book Encyclopedia* Vol 21 (World Book, Inc, Chicago, 2002)**

The World Book Encyclopedia **Vol 4 (World Book, Inc, Chicago, 2002)**

Tugendhat and Christie (ed) ***The Law of Privacy and the Media***

Tugendhat M and Christie I (ed) *The Law of Privacy and the Media* (Oxford University Press 2002)

Turn ***Transborder Data Flows: Concerns in Privacy Protection and Free Flow of Information***

Turn R (ed) *Transborder Data Flows: Concerns in Privacy Protection and Free Flow of Information* Vol 1-2 (American Federation of Information Processing Societies, 1979)

U

Umozurike 1988 (1) ***Afr J Intl L*** **65**

Umozurike U O "The Protection of Rights Under the Banjul (African) Charter on Human and People's Rights" *African Journal of International Law* Vol 1 no 1 (1988) 65-83

Umozurike 1983 (77) ***AJIL*** **(1983) 902**

Umozurike U O "The African Charter on Human and Peoples' Rights" 77 *American Journal of International Law* (1983) 902-912

V

Veljanovski "The Economics of Regulatory Enforcement"

Veljanovski C G "The Economics of Regulatory Enforcement" 171-188 in Hawkins K and Thomas J (eds) *Enforcing Regulation* (1984)

Vogel ***Trading Up: Consumer and Environmental Regulation in a Global Economy***

Vogel D *Trading Up: Consumer and Environmental Regulation in a Global Economy* (Harvard University Press, 1997)

W

Wacks *Law, Morality and the Private Domain*

Wacks R *Law, Morality and the Private Domain* (Hong Kong University Press, 2000)

Wacks *Personal Information: Privacy and the Law*

Wacks R *Personal Information: Privacy and the Law* (Oxford University Press, USA, 1993)

Wacks *Privacy*

Wacks R *Privacy* (Dartmouth, London, 1993)

Wacks 1980 (96) *L Q R* 73

Wacks R "The Poverty of 'Privacy" Vol 96 *Law Quarterly Review* (1980) 73- 89

Waldo, Lin and Millett (eds) *Engaging Privacy and Information Technology in a Digital Age*

Waldo J, Lin H S and Millett L I (eds) *Engaging Privacy and Information Technology in a Digital Age* (National Academy Press, 2007)

Walczuch, Singh and Palmer 1995 (8) No 2 *Inform Tech & People* 37

Walczuch R M, Singh S. K. and Palmer T S "An Analysis of the Cultural Motivations for Trans-border Data Flow Legislation" *Information Technology & People* Vol 8 No 2 (1995) 37-57

Warren and Brandeis 1890 (4) *Harv L Rev* 193

Warren S D & Brandeis L "The Right to Privacy" 1890 (4) *Harvard Law Review* 193-220

Webb 2003 (2) *JILT* 5

Webb P "A Comparative Analysis of Data Protection Laws in Australia and Germany" 2 *Journal of Information, Law and Technology* (JILT) Issue No 2 (2003)

Welch and Meltzer *Human Rights and Development in Africa: Dilemmas and Options*

Welch E C and Meltzer R I (eds) *Human Rights and Development in Africa: Dilemmas and Options* (State University of New York Press, 1984)

Weller and Shaffer *2008 (26) Association of Corporate Counsel Docket* 88

Weller M and Shaffer R *"*Making a Federal Case Out of Employee Theft of Trade Secrets*"* *Association of Corporate Counsel Docket Vol 26 No 8 (2008)* 88-99

Westby *International Guide to Privacy*

Westby J R *International Guide to Privacy* (American Bar Association, 2004)

Westin *Privacy and Freedom*

Westin A *Privacy and Freedom* (Bodley Head 1970)

Wilson and Al-Muhanna" 1985 (22) *J Peace Res* 289

Wilson L J and Al-Muhanna I "The Political Economy of Information: The Impact of Transborder Data Flows" *Journal of Peace Research* Vol 22 No 4 (1985) 289-301

Winn "The Emerging Law of Electronic Commerce"

Winn J K "The Emerging Law of Electronic Commerce" 691-710 in Shaw M, Blanning R, Strader T & Winston A (eds) *Handbook on Electronic Commerce* (Springer, 2000)

Wright and Kakalik 1997 (27) No 4 *Computers and Society* 22

Wright M and Kakalik J "The Erosion of Privacy" *Computers and Society* Vol 27 No 4 (1997) 22-26

Wriston 1997 (76) *Foreign Affairs* 172

Wriston W "Bits, Bytes, and Diplomacy" Vol 76 No 5 *Foreign Affairs* (1997) 172–182

Wyatt "Freedom of Expression in the EU Legal Order and in EU Relations with Third Countries"

Wyatt D "Freedom of Expression in the EU Legal Order and in EU Relations with Third Countries" in Beatson J and Cripps Y (ed) *Freedom of Expression and Freedom of Information, Essays in Honour of Sir David William* (Oxford University Press, 2000)

Z

Zinser 2003 (21) *J Marshall J Computer & Info L* 547

Zinser A "International Data Transfer Out of the European Union: The Adequate Level of Data Protection According to Article 25 of the European Data Directive" *John Marshall Journal of Computer and Information Law* Vol 21 No 4 (2003) 547-565

ONLINE (INTERNET) SOURCES: ARTICLES, STUDIES, REPORTS, POLICY DOCUMENTS AND WEBSITES

A

Abati *Revolt of the South-South*

Abati R *Revolt of the South-South* (2005).

Available at <http://www.nigeriavillagesquare.com/articles/reuben-abati/revolt-of-the-south-south-14.html> [Accessed on 10/3/13]

Access Bank Plc website

Available at <http://www.accessbankplc.com/pages/Page.aspx?Value=161&ln=Gy7UlI4c-SJE94Wa2qudbFQ%3d%3d> [Accessed 25/5/13]

ACCI *Extraterritorial Application of National Laws*

Australian Chamber of Commerce and Industry *The Extraterritorial Application of National Laws: An Unwarranted Burden for International Business* (Issues Paper) (2006)
Available at <http://www.cacci.org.tw/Journal/2006%20Vol%202/Extraterritorial.pdf> [Accessed 20/4/13]

ACP-EC website (referring to Lome Convention)

Available at <http://www.acpsec.org/content/lome-convention> [Accessed 3/3/13]

African Development Bank Group *Nigeria Country Strategy Paper*

African Development Bank Group *Federal Republic of Nigeria Country Strategy Paper 2013-2017* (ORWA Deptartment 2013)

Available at <http://www.afdb.org/en/countries/west-africa/nigeria/nigeria-economic-outlook/> [Accessed 10/3/13]

Akdeniz 2001 (3) *EBLR* 110

Akdeniz Y "Case Analysis of League against Racism and Anti-semitism (Licra)" *Electronic Business Law Reports* 1 (3) (2001) 110-120

Available at <http://www.cyber-rights.org/documents/yahoo_ya.pdf > [Accessed 3/5/08]

Alabi *Empowering Socio-Economic Development in Africa*

Alabi G A *Empowering Socio-Economic Development in Africa*: *Utilizing Information Technology: A Critical Examination of the Social, Economic, Technical and Policy Issues in Nigeria* AISI Case Study (1996)

Available at <http://repository.uneca.org/handle/10855/10366 > [Accessed 4/5/13]

ALRC *For Your Information*

Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*

Available at <http://www.alrc.gov.au/publications/report-108> [Accessed 30/5/13]

Andersen and Babula "Openness and Long-Run Economic Growth"

Andersen L and Babula R "The Link Between Openness and Long-Run Economic Growth*"* in United States International Trade Commission *Journal of International Commerce and Economics* (Web version) (2008)

Available at <http://www.usitc.gov/publications/332/journals/openness_growth_link.pdf>. [Accessed 24/5/13]

Anti-phishing Working Group website

Available at <www.antiphishing.org> [Accessed 25/5/13]

Anya *When will Nigeria take Charge of Nigeria?*

Anya O A *When will Nigeria take Charge of Nigeria?* (Lecture under the auspices of the Gindiri Old Boys Association, Hill Station Hotel, Jos, Plateau State, Nigeria on November 6, 2004)

Available at <http://www.dawodu.com/anya1.htm> [Accessed on 10/3/13]

APEC Privacy Framework website

Available at <http://publications.apec.org/publication-detail.php?pub_id=390> [Accessed 12/10/12]

Apte and Nath *Size, Structure and Growth of the US Information Technology*

Apte U M and Nath H K *Size, Structure and Growth of the US Information Technology* (2004)

Available at <http://www.anderson.ucla.edu/documents/areas/ctr/bit/ApteNath.pdf.pdf>. [Accessed 11/3/13]

B

Baker and Miller "Privacy, Anti-Trust and the National Information Infrastructure"

Baker D I and Miller W T "Privacy, Anti-Trust and the National Information Infrastructure: Is Self-Regulation of Telecommunications-Related Personal Information a Workable Tool?" in NTA *Privacy and Self-Regulation in the Information Age* (1997)
Available at <http://www.ntia.doc.gov/page/chapter-2-antitrust-considerations> [Accessed 30/5/13]

Bakibinga *Electronic Privacy in the Telecommunications Sub-sector*

Bakibinga E M *Managing Electronic Privacy in the Telecommunications Sub-sector: The Ugandan Perspective*. Paper presented at Africa Electronic Privacy and Public Voice Symposium, (2004)
Available at: <http://thepublicvoice.org/events/capetown04/bakibinga.ppt> [Accessed 14/7/05]

BBC News "Tracking a suspect by mobile phone"

British Broadcasting Corporation *The BBC News* "Tracking a suspect by mobile phone" *News* (3rd August 2005).
Available at <http://news.bbc.co.uk/2/hi/technology/4738219.stm> [Accessed 13/3/13]

BBC *News* "Facebook sex abuser"

British Broadcasting Corporation *The BBC News* "Facebook sex abuser Jake Ormerod jailed for 10 years" (8 July 2011)

Available at <http://www.bbc.co.uk/news/uk-england-devon-14082306>. [Accessed 25/10/12]

Bennett *International Standard for the Protection of Personal Information*

Bennett C J *Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada* (1997)

Available at <http://www.ilpf.org/events/jurisdiction2/presentations/bennett_pr/> [Accessed 19/4/13]

Bennett *Privacy in the Political System*

Bennett C J *Privacy in the Political System: Perspectives from Political Science and Economics*

Available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2230389>. [Accessed 30/3/13]

Black "Forms and Paradoxes of Principles Based Regulation"

Black J "Forms and Paradoxes of Principles Based Regulation" in London School of Economics *Law, Society and Economy Working Papers* 13/2008

Available at <http://ssrn.com/abstract=1267722> [Accessed 1/6/13]

Board of Governors *Availability of Consumer Identifying Information*

Board of Governors of the Federal Reserve System *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 2 (March 1997), quoted in Prepared Statement of Fred H Cate before the Subcommittee on Courts and Intellectual Property, Committee of the Judiciary, US House of Representatives, presented March 26, 1998

Available at <http://www.fas.org/irp/congress/1998_hr/h980326cf.htm> [Accessed 21/5/13]

Branscomb *Economics of Information*

Branscomb A W *The Economics of Information: Public and Private Domains of Information: Defining the Legal Boundaries* (1994)

Available at <http://www.asis.org/Bulletin/Dec-94/branscomb.html> [Accessed 17/7/12]

Brown and Stern *Global Market Integration and National Sovereignty*

Brown A G and R M Stern *Global Market Integration and National Sovereignty* (Research Seminar in International Economics Discussion Paper No 518) (2004)

Available at <http://www.fordschool.umich.edu/rsie/workingpapers/Papers501-525/r518-.pdf> [Accessed 23/5/13]

C

Castells *Information Technology, Globalization and Social Development*

Castells M *Information Technology, Globalization and Social Development* (1999) UNRISD Discussion Paper No 114

Available at < http://www.unrisd.org> [Accessed 3/10/13]

Cate "The Failure of Fair Information Practice Principles"

Cate F H "The Failure of Fair Information Practice Principles" 341-378 in *Consumer Protection in the Age of the "Information Economy"*

Available at: <http://www.hunton.com/files/tbl_s47Details/FileUpload265/1248/Failure_of_-Fair_Information_Practice_Principles.pdf> [Accessed 21/5/13]

Cavoukian *Data Mining: Staking a Claim on your Privacy*

Cavoukian A *Data Mining: Staking a Claim on your Privacy* (1998)

Available at <http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=342> [Accessed 20/4/13]

Central Bank of Nigeria *Guidelines on Electronic Banking*

Central Bank of Nigeria *Guidelines on Electronic Banking in Nigeria* 2003

Available at <http://www.cenbank.org/OUT/PUBLICATIONS/BSD/2003/E-BANKING.-PDF> [Accessed 4/5/13]

Central Bank of Nigeria *Report of the Technical Committee on Electronic Banking*

Central Bank of Nigeria Report of the Technical Committee on Electronic Banking, 2003 Available at <http://www.cenbank.org/out/publications/BSD/2003/E-BANKINGRPT.PDF> [Accessed 4/5/13]

Central Bank of Nigeria (CBN) website

Available at <http://www.cenbank.org/rates> [Accessed 10/3/13]

CHRI *Looking for the Right to Information in the Commonwealth*

Commonwealth Human Rights Initiative *Looking for the Right to Information in the Commonwealth* (2003)
Available at: <http://www.humanrightsinitiative.org/publications/chogm/chogm_2003/-default.htm> [Accessed 4/3/13]

CIA *World Fact Book* (2011)

Central Intelligence Agency *World Fact Book* (2011)

Available at <https://www.cia.gov/library/publications/the-world-factbook/geos/ni.html> [Accessed 4/3/13]

Citigroup *Review of the EU Data Protection Directive*

Citigroup *Review of the EU Data Protection Directive* (22 August 2002)

Available at <http://ec.europa.eu/justice/policies/privacy/docs/lawreport/paper/citigroup_-en.pdf> [Accessed 21/5/13]

Clarke *Introduction to Dataveillance*

Clarke *R Introduction to Dataveillance and Information Privacy and Definition of Terms* (2005)

Available at <http://www.rogerclarke.com/DV/Intro.html> [Accessed 2/6/12]

Clinton *Presidential Directive on E-Commerce*

Clinton W J *Presidential Directive on E-Commerce* (July 1, 1997)

Available at <https://www.fas.org/irp/offdocs/pdd-nec-ec.htm > [Accessed 30/5/13]

Cogburn and Adeya "Understanding Globalisation and the Information Economy"

Cogburn D L and Adeya C N "Understanding Globalisation and the Information Economy" 1-10 in *Globalization and the Information Economy: Challenges and Opportunities for Africa* (1999)

Available at <http://www.unu.edu/africa/papers/cogburn-adeya.pdf> [Accessed 9/3/13]

Coglianese, Healey, Keating and Michael "The Role of Government in Corporate Governance"

Coglianese C, Healey T J, Keating E K and Michael M L "The Role of Government in Corporate Governance" in *Regulatory Policy Program Report* (RPP-08) (2004)

Available at <http://www.hks.harvard.edu/m-rcbg/research/rpp/reports/RPPREPORT8.pdf> [Accessed 1/6/13]

Coughlan, Currie, Kindred and Scassa *Global Reach, Local Grasp*

Coughlan S, Currie R J, Kindred H M and Scassa T *Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization* (Paper prepared for the Law Commission of Canada 2006)

Available at <www.library.dal.ca/law/Guides/FacultyPubs/Joint/GlobalReachFinal.pdf>. [Accessed 20/4/13]

Consumer Affairs Bureau (Nigeria) website

Available at <http://ncc.gov.ng/archive/index3.htm> [Accessed 15/3/13]

Council of Economic Advisers *Economic Report of the President*

Council of Economic Advisers (USA) *Economic Report of the President* (2004)

Available at <http://www.presidency.ucsb.edu/economic_reports/2004.pdf> [Accessed 20/3/13]

D

Data Guidance *UN Resolution to Establish International Human Right to Privacy Online*

Available at <http://www.dataguidance.com/news.asp?id=2151> [Accessed 31/12/13]

Data Protection Commissioner of Ireland *Frequently Asked Questions*

Available at <http://www.dataprotection.ie/viewdoc.asp?DocID=1240&UserLang=EN> [Accessed 19/4/13]

Data Protection and Privacy Commissioners Montreux Declaration

Data Protection and Privacy Commissioners 27th International Conference (Montreux, Switzerland, 14-16 September 2005)

Available at <http://www.privacyconference2005.org/> [Accessed 25/5/13]

De Boni and Prigmore *Privacy and the Information Economy*

De Boni M and Prigmore M *Privacy and the Information Economy* (2003)

Available at <http://el.trc.gov.om:4000/htmlroot/ENGG/tcolon/e_references/Consolidated/-Information%20and%20Technology%20Engineering/Journals/Privacy%20and%20the%20-information%20economy.pdf> [Accessed 30/3/13]

DeCew *Privacy*

DeCew J "Privacy" in Zalta E N (ed) *The Stanford Encyclopedia of Philosophy* (2002)

Available at <http://plato.stanford.edu/entries/privacy/> [Acessed 20/3/13]

Dempsey 1997 (8) No 1 *Albany Law J Sci Technol*

Dempsey J X "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy" *Albany Law Journal of Science & Technology*, Vol 8, No 1, (1997)

Available at <http://www.cdt.org/publications/lawreview/1997albany.shtml> [Accessed 15/4/13]

DeRosa *Data Mining and Data Analysis for Counterterrorism*

DeRosa M *Data Mining and Data Analysis for Counterterrorism* (2004)

Available at <http://www.cdt.org/security/usapatriot/20040300csis.pdf> [Accessed 27/7/12]

Dignan "FBI, Feds collect Facebook, social media data; why are you surprised?"

Dignan L "FBI, Feds collect Facebook, social media data; why are you surprised?" in *Between the Lines (Zdnet Blog)* (17 March 2010)

Available at <http://www.zdnet.com/blog/btl/fbi-feds-collect-facebook-social-media-data-why-are-you-surprised/31996> [Accessed 15/10/12]

Dixon *Australia's New Privacy Legislation*

Dixon T *Australia's New Privacy Legislation* Baker & McKenzie Cyberspace Law and Policy Centre Continuing Legal Education Conference (24-25 May 2001)
Available at: <http://www.cyberlawcentre.org/Articles/Cyberspace_May_2001/Privacy_.2001.html> [Accessed 30/5/13]

Dixon *Introduction to Fair Information Practices*

Dixon P *A Brief Introduction to Fair Information Practices*
Available at: http://www.worldprivacyforum.org/fairinformationpractices.html > [Accessed 21/5/13]

Domesday Book
Available at <http://www.domesdaybook.co.uk> [Accessed 15/4/13]

Drake *ICT Global Governance and the Public Interest*

Drake W J *ICT Global Governance and the Public Interest: Transactions and Content Issues* (2004) 6
Available at <http://katrinaresearchhub.ssrc.org/ict-global-governance-and-the-public-interest-transactions-and-content-issues/attachmentu> [Accessed 20/4/13]

Duthiers *CNN News* "Facebook 'stalkers' face trial for model's murder"

Duthiers V "Facebook 'stalkers' face trial for model's murder" CNN (October 26, 2012)
Available at <http://edition.cnn.com/2012/10/25/world/africa/nigeria-facebook-murder-cynthia-osokogu/index.html> [Accessed 26/10/12]

E

Economist* magazine *The 2005 E-Readiness Rankings

Economist magazine (Intelligence Unit) *The 2005 E-Readiness Rankings*
Available at <http://www.eiu.com> [Accessed 12/6/12]

Economist magazine (Intelligence Unit) ***Digital Economy Rankings 2010***

Economist magazine (Intelligence Unit) *Digital Economy Rankings 2010: Beyond E-Readiness Report* (2010)

Available at: <http://graphics.eiu.com/upload/EIU_Digital_economy_rankings_2010_-FINAL_WEB.pdf> [Accessed 5/4/13]

EGA Position Paper ***TRIPS Article 39.3 does not require Data Exclusivity Provisions***

European Generic Medicines Association (EGA) Position Paper *TRIPS Article 39.3 does not require Data Exclusivity Provisions* (2000)

Available at <http://198.170.119.137/doc/ega_trips39.3_2000.pdf> [Accessed 26/5/13]

European Commission ***Trade (website)***

Available at <http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/> [Accessed 5/4/13]

European Commission ***Decisions on adequacy***

European Commission *Decisions on the adequacy of the protection of personal data in third countries*

Available at <http://ec.europa.eu/justice/data-protection/document/international-transfers/-adequacy/index_en.htm> [Accessed 25/5/13]

European Commission Press Release ***EU approves New Zealand's data protection standards in step to boost trade***

Available at http://europa.eu/rapid/press-release_IP-12-1403_en.htm [Accessed 25/5/13]

European Union ***Trade with the World and EU Trade with Nigeria***

Available at <http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_113427.pdf> [Accessed 10/4/13]

EPIC ***Computer Security Act***

Electronic Privacy Information Center page on the Computer Security Act of 1987

Available at <http://epic.org/crypto/csa/> [Accessed 30/5/13]

EPIC *Privacy and Consumer Profiling*

Electronic Privacy Information Center page on Consumer Profiling

Available at: <http://www.epic.org/privacy/profiling/> [Accessed 4/3/13]

EPIC *Amicus Curiae brief in Estate of Helen Remsburg*

Electronic Privacy Information Center *Amicus Curiae brief in case no C-00-211B Estate of Helen Remsburg v Docusearch, Inc, et al* (2002)

Available at <http://www.epic.org/privacy/boyer/brief.html> [Accessed 26/9/12]

Esselaar, Gillwald and Stork *Towards an African e-Index 2007*

Esselaar S, Gillwald A and Stork C *Towards an African e-Index 2007: Telecommunications Sector Performance in 16 African Countries: A Supply-side Analysis of Policy Outcomes* (2007)

Available at: <http://www.researchictafrica.net/publications/Research_ICT_Africa_e-Index_-Series/Telecommunication%20Sector%20Performance%20in%2016%20African%20-Countries%20-%20a%20supply-side%20analysis%20of%20policy%20outcomes.pdf> [Accessed 13/3/13]

Eurostat website *EU Population*

European Commission Eurostat website *EU Population*

Available at <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&language=en&-pcode=tps00001&tableSelection=1&footnotes=yes&labeling=labels&plugin=1>. [Accessed 3/3/13]

Export.gov website

Available at <http://export.gov/safeharbor/ > [Accessed 5/4/13]

F

FATF *Annual Review 2006-2007*

Financial Action Task Force *Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review*

Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/2006%202007%20-NCCT%20ENG.pdf> [Accessed 6/3/13]

FBI *Internet Fraud Report* 2001/ 2002

FBI *Internet Fraud and Complaints Center Report* 2001/ 2002

Available at: <http://www.fbi.gov/scams-safety/fraud/internet_fraud > [Accessed 3/3/13]

FBI *The Insider Threat*

Federal Bureau of Investigation (FBI) *The Insider Threat: An introduction to Detecting and Deterring an Insider Spy*

Available at: <http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat> [Accessed 19/8/12]

FCA *Handbook*

Financial Conduct Authority (UK) *Handbook*

Available at <http://fshandbook.info/FS/html/FCA/> [Accessed 1/6/13]

FDIC *Offshore Outsourcing*

Federal Deposit Insurance Corporation (US) *Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks* (2004)

Available at <http://www.fdic.gov/regulations/examinations/offshore/index.html> [Accessed 20/3/13]

First City Monument Bank website

Available at <http://www.fcmb.com/privacy-policy>]Accessed 25/5/13]

Freedom of Information Coalition website

Available at <http://www.foicoalition.org/foi_bill/index.htm> [Accessed 4/3/13]

Freedom of Information Coalition *Memorandum on the Freedom of Information Bill*

Freedom of Information Coalition *Memorandum on the Freedom of Information Bill* (2005) Available at: <http://www.humanrightsinitiative.org/programs/ai/rti/international/laws_-papers/nigeria/Memo%20submitted%20to%20FOI%20Committee.pdf> [Accessed 15/4/13]

FSA website

Financial Services Authority (UK) website
Available at <http://www.fsa.gov.uk/about/who/history> [Accessed 1/6/13]

FTC website

Federal Trade Commission (USA) website
Available at <http://www.ftc.gov/privacy/index.html> [Accessed 30/5/13]

FTC Report *Protecting Consumer Privacy*

Federal Trade Commission Report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012)
Available at <http://ftc.gov/os/2012/03/120326privacyreport.pdf> [Accessed 20/4/13]

FTC *Self-regulation and Privacy Online*

Federal Trade Commission *Self-regulation and Privacy Online: A Report to Congress* (July 1999)
Available at <http://www.ftc.gov/os/1999/07/privacy99.pdf> [Accessed 30/5/13]

G

Gellman *Fair Information Practices*

Gellman R *Fair Information Practices: A Basic History* (2011)
Available at <http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.> [Accessed 20/3/13]

Gibson "Globalization and the Technology Standards Game"

Gibson C S "Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards" *Suffolk University Law School Legal Studies Research Paper No. 07-39*
Available at <http://ssrn.com/abstract=1010125> [Accessed 23/5/13]

Gindin *Guide to E-mail and the Internet in the Workplace*

Gindin S *Guide to E-mail and The Internet in the Workplace* (Bureau of National Affairs Inc, 1999))

Available at <http://www.info-law.com/guide.html> [Accessed 9/3/13]

Gleick "Big Brother Is Us"

Gleick J "Big Brother Is Us" *New York Times* (29th September 1996)

Available at: <http://www.nytimes.com/1996/09/29/magazine/big-brother-is-us.html?page-wanted=all&src=pm> [Accessed 23/4/13]

Gow *Improving Identity Check Processes*

Gow G A *Improving Identity Check Processes for Pre-paid Mobile Services: Comments submitted to Australian Communications and Media Authority* (2006) 13

Available at <http://www.acma.gov.au/webwr/_assets/main/lib100696/dr%20gordon%20-gow.pdf> [Accessed 13/3/13]

Gow *Privacy and Ubiquitous Network Societies*

Gow G A *Privacy and Ubiquitous Network Societies*. Background Paper for the ITU Workshop on Ubiquitous Network Societies, Doc UNS/05 (April 2005)

Available at <http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20-paper.pdf> [Accessed 20/11/05]

Greenleaf 2011 No 112 *PL&BIR*

Greenleaf G "Global Data Privacy Laws: Forty Years of Acceleration" *Privacy Laws and Business International Report* No 112 (2011)

Available at <http://ssrn.com/abstract=1946700> [12/7/12]

Greenstadt and Smith *Protecting Personal Information*

Greenstadt R and Smith M D *Protecting Personal Information: Obstacles and Directions* (2005). Fourth Workshop on the Economics of Information Security (WEIS05) 2005

Available at <http://infosecon.net/workshop/pdf/48.pdf> [Accessed 2/6/13]

Greenstein "Commercialization of the Internet"

Greenstein S "Commercialization of the Internet: The Interaction of Public Policy and Private Choices or Why Introducing the Market Worked So Well" in Jaffe J B, Lerner J and Stern S (ed) *Innovation Policy and the Economy* Vol 1 (MIT Press 2001) 151

Available at <http://www.nber.org/chapters/c10779.pdf?new_window=1> [Accessed 8/3/13]

Grossman and Helpman "Technology and Trade"

Grossman G M and Helpman E "Technology and Trade" (1994) *NBER Working Paper Series no 4926*

Available at <http://www.nber.org/papers/w4926> [Accessed 24/5/13]

The Guardian newspaper (Nigeria) website

Available at <http://www.ngrguardiannews.com> [Accessed 13/3/13]

The Guardian newspaper (UK) *NSA Files*

Available at <http://www.theguardian.com/world/the-nsa-files> [Accessed 17/1/14]

Guazelli *Predicting the future*

Alex Guazelli *Predicting the future, Part 1: What is predictive analytics?* (2012)

Available at <http://www.ibm.com/developerworks/industry/library/ba-predictive-analytics1-/index.html> [Accessed 30/5/13]

H

Hakkio *Economic Policy for the Information Economy*

Hakkio C S *Economic Policy for the Information Economy: A Summary of the Bank's 2001 Economic Symposium* Federal Reserve Bank of Kansas City (2001)

Available at <http://www.kansascityfed.org/publications/research/er/er-2001.cfm>. [Accessed 8/3/13]

Hamelink ***New Information and Communication Technologies***

Hamelink C J *New Information and Communication Technologies, Social Development and Cultural Change* (UNRISD) Discussion Paper No 86 (1997)

Available at: <http://www.unrisd.org/unrisd/website/document.nsf/0/398D6A861127084780-256B640051A497?OpenDocument> [Accessed 13/11/12]

Hamilton ***September 11***

Hamilton S *September 11, the Internet, and the Effects of Information Provision in Libraries* (2002) Paper presented at the 68th IFLA Council and General Conference, Glasgow (18–24 August 2002)

Available at <http://www.ifla.org/IV/ifla68/papers/156-079e.pdf> [20/4/13]

Hans-Bredow Institut ***Final Report***

Hans-Bredow Institut *Final Report: Study on Co-Regulation Measures in the Media Sector* Study for the European Commission, Directorate Information Society and Media on co-regulation (2006)

Available at <http://ec.europa.eu/avpolicy/docs/library/studies/coregul/final_rep_en.pdf>. [Accessed 30/5/13]

Harvard University Center ***Global Information Technology Report***

Harvard University Center for International Development *The Global Information Technology Report 2001-2002* (2002)

Available at <http://www.cid.harvard.edu/archive/cr/gitrr_030202.html> [Accessed 4/5/13]

Heisenberg ***Can the European Union Control the Agenda of Globalization?***

Heisenberg D *Can the European Union Control the Agenda of Globalisation?* (2004)
Available at: <http://martindale.cc.lehigh.edu/sites/martindale.cc.lehigh.edu/files/heisenberg.pdf> [Accessed 25/5/13]

Henry ***et al Emerging Digital Economy***

Henry D, Cook, S, Buckley P, Dumagan J, Gurmuk G and Pastore D (US Department of Commerce) *The Emerging Digital Economy II*

Available at <http://www.pubklaw.com/papers/ede2.pdf> [Accessed10/3/13]

Hirsch *Law and Policy of Online Privacy*

Hirsch D *The Law and Policy of Online Privacy: Regulation, Self-regulation, or Co-regulation?*

Available at: <http://works.bepress.com/dennis_hirsch/1> [Accessed 30/5/13]

Hoekman and Braga *Protection and Trade in Services*

Hoekman B and Braga C A *Protection and Trade in Services: A Survey* (World Bank Policy Research Working Paper No 1747 1997)

Available at <http://ssrn.com/abstract=569236> [Accessed 5/3/13]

Huffaker and Calvert 2005 (10) No 2 *JCMC* 63

Huffaker D A and Calvert S L "Gender, Identity, and Language Use in Teenage Blogs" Journal of Computer-Mediated Communication. *Journal of Computer-Mediated Communication* Vol 10 No 2 (2005)

Available at <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2005.tb00238.x/full> [Accessed 9/3/13]

Hufbauer and Warren *Globalisation of Services*

Hufbauer G and Warren T *The Globalisation of Services: What Has Happened? What Are the Implications?* (1999)

Available at <http://www.iie.com/publications/wp/99-12.pdf.> [Accessed 9/3/13]

I

ICC *Extraterritoriality and Business*

International Chamber of Commerce *Extraterritoriality and business* (Policy Statement) (2006)

Available at <http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2006/-Extraterritoriality-and-business/> [Accessed 1/5/13]

ICO *Data Protection Regulatory Action Policy*

Information Commissioner's Office (UK) *Data Protection Regulatory Action Policy* (2004)

Available at <http://www.ico.org.uk/about_us/~/media/documents/library/Data_Protection/-Detailed_specialist_guides/data-protection-regulatory-action-policy.pdf> [Accessed 12/9/13]

IDRC *Acacia Initiative*

IDRC *Acacia Initiative*

International Development Research Centre *Acacia Initiative*

Available at <http://web.idrc.ca/ev.php?ID=5895_201&ID2=DO_TOPIC [Accessed 10/3/13]

Ige *Evolution of the Telecommunications Industry*

Ige O *Evolution of the Telecommunications Industry* (2003).

Available at <http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=-589:speeches&catid=72:cat-web-speeches&Itemid=93> [Accessed 4/5/13]

IICD website

International Institute for Communication and Development website

Available at <http://www.iicd.org> [Accessed 10/3/13]

IITF (US) *National Information Infrastructure*

Information Infrastructure Task Force Report (US) *National Information Infrastructure: Agenda for Action* (1993)

Available at <http://www.ibiblio.org/nii/toc.html> [Accessed 5/4/13]

In the Matter of the Application of the USA for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government

In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government. (Gov App 5, Docket No 3)

Available at: <https://www.eff.org/files/filenode/celltracking/criminalapplicationorder_-finalopinion.pdf> [Accessed 3/1/12]

Irving *Privacy Report*

Irving L *Privacy Report: Introduction* (NTIA) (1997)
Available at <http://www.ntia.doc.gov/page/privacy-report-introduction> [Accessed 20/9/11]

ISPA *Spam*

Internet Service Providers Association of South Africa *Spam*
Available at<http://ispa.org.za/spam/> [Accessed 20/4/13]

ITG *Readiness for the Networked World*

Information Technologies Group *Readiness for the Networked World: A Guide for Developing Countries*
Available at <http://cyber.law.harvard.edu/readinessguide/readiness.html> [Accessed 2/3/13]

Iyoha and Oriakhi *Explaining African Economic Growth*

Iyoha M A and Oriakhi D *Explaining African Economic Growth Performance: The Case of Nigeria* (2002)
Available at <http://www.gdnet.org/~research_papers/Explaining%20African%20economic-%20growth%20performance:%20the%20case%20of%20Nigeria> [Accessed 10/3/13]

J

Jakobsson *Human Factor in Phishing*

Jakobsson M *The Human Factor in Phishing*
Available at <http://markus-jakobsson.com/papers/jakobsson-psci07.pdf> [Accessed 25/5/13]

K

Kierkegaard 2005 (1) *Shidler JL Com & Tech*

Kierkegaard S M "Safe Harbor Agreement: Boon or Bane?" *Shidler Journal for Law, Commerce & Technology* Vol 1 No 3 (2005)
Available at < http://www.lctjournal.washington.edu/vol1/a010Kierkegaard.html> [Accessed 25/5/13]

Kigongo *Concepts of Individuality and Social Cohesion*

Kigongo J K *The Concepts of Individuality and Social Cohesion: A Perversion of Two African Cultural Realities*

Available at <http://www.crvp.org/book/series02/11-2/chapter_iv.htm > [Accessed 3/4/13]

Kobrin *Trans-Atlantic Data Privacy Dispute*

Kobrin S J *The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance* (2002)

Available at: <http://ssrn.com/abstract=349561>. [Accessed 20/4/13]

Kuner *Regulation of Transborder Data Flows*

Kuner C "*Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*" Tilburg University Legal Studies Working Paper No 016 (2010)

Available at <http://ssrn.com/abstract=1689483> [Accessed 20/4/13]

L

Law Reform Commission of Ireland *Report*

Law Reform Commission of Ireland *Report*: *Surveillance and the Interception of Communications* (1998)

Available at: <http://www.lawreform.ie/_fileupload/Reports/rPrivacy.htm> [Accessed 4/4/13]

Leiner, Cerf, Clark *Brief History of the Internet*

Leiner B M, Cerf V G, Clark D D, Kahn R E, Kleinrock L, Lynch D C, Postel J, Roberts L G and Wolff S *Brief History of the Internet* (2003)

Available at <http://www.internetsociety.org/brief-history-internet> [Accessed 7/3/13]

Leith 1997 *JILT*

Leith P "Shamans, Software and Spleens: Law and the Construction of the Information Society" *Journal of Information Law & Technology* (1997).

Available at <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_2/leith2/>. [Accessed 4/3/13]

Litan *Law and Policy in the Age of the Internet*

Litan R E *Law and Policy in the Age of the Internet* AEI-Brookings Joint Centre Working Paper No 01-4 (2001)
Available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=286358> [Accessed 30/5/13]

Lloyd and Sreedhar "Hobbes's Moral and Political Philosophy"

Lloyd S A and Sreedhar S "Hobbes's Moral and Political Philosophy" in Zalta E N (ed) *The Stanford Encyclopedia of Philosophy* (Summer 2013 edition)
Available at <http://plato.stanford.edu/archives/sum2013/entries/hobbes-moral/> [Accessed 30/3/13]

Longworth *Transborder Data Flow*

Longworth E *Transborder Data Flow: EU Directive and Implications for International Business*
Available at <www.pcpd.org.hk/english/infocentre/files/nz_3.doc> [Accessed 13/4/13]

Loukidelis *Transborder Data Flows and Privacy*

Loukidelis D *Transborder Data Flows and Privacy – An Update on Work in Progress* (2006)
Available at: <http://www.oipcbc.org/pdfs/Speeches/TransborderDataFlowsSpeech-(10Feb06).pdf> [Accessed 5/4/13]

M

Mamora *Why Obasanjo Refused to Sign FOI Act*

Mamora O *Why Obasanjo Refused to Sign FOI Act – Mamora* (2011)
Available at <http://actioncongressnigeria.org/2011/11/22/why-obasanjo-refused-to-sign-foi-act-–-mamora/> [Accessed 15/4/13]

Mankiw and Swagel *The Politics and Economics of Offshore Outsourcing*

Mankiw and Swagel *The Politics and Economics of Offshore Outsourcing*
Available at: <http://www.nber.org/papers/w12398> [Accessed 10/3/13]

Mann *Electronic Commerce in Developing Countries*

Mann C L *Electronic Commerce in Developing Countries: Issues for Domestic Policy and WTO Negotiations* (2000)

Available at < http://xxx.iie.com/publications/wp/00-3.pdf> [Accessed 10/3/13]

Manyika and Roxburgh *The Great Transformer*

Manyika J and Roxburgh C (McKinsey Global Institute) *The Great Transformer: How the Internet is Changing the Globe and its Citizens* (2011)

Available at <http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_-transformer> [Accessed 7/4/13]

Mason *Tapestry of Privacy*

Mason R O *Tapestry of Privacy* (A Meta-Discussion)

Available at <http://cyberethics.cbi.msstate.edu/mason2/coda.htm > [Accessed 20/3/13]

Mattoo *Economics and Law of Trade in Services*

Mattoo A *Economics and Law of Trade in Services* (2005)

Available at <http://siteresources.worldbank.org/INTRANETTRADE/Resources/Topics/-Accession/Economics&LawOfTradeInServices_Mattoo.pdf> [Accessed 9/3/13]

Mattoo and Wunsch *Preempting Protectionism in Services*

Mattoo A and Wunsch S *Preempting Protectionism in Services: The GATS and Outsourcing* (2004)
Available at <www.iie.com/publications/papers/wunsch0204.pdf> [Accessed 7/3/13]

Mendel *Freedom of Information: A Comparative Legal Survey*

Mendel T *Freedom of Information: A Comparative Legal Survey* (UNESCO, 2003)

Available at: <http://www.unesco.org/new/en/communication-and-information/resources-/publications-and-communication-materials/publications/full-list/freedom-of-information-a-comparative-legal-survey/> [Accessed 15/4/13]

Ministry of Communications Technology (Nigeria) website

Available at at: <http://www.commtech.gov.ng/index.php/the-ministry/about-the-ministry/> [Accessed 12/3/13]

Molla *Africa and the Information Economy*

Molla A *Africa and the Information Economy: Foundations, Opportunities, Challenges and Research Agenda* (2000)

Available at <http://www.uneca.org/AKNF/pub/informationeconomy.PDF> [Accessed 4/5/13]

Mortgage Introducer *Law Society Critical of Principle-Based Approach*

Mortgage Introducer *Law Society Critical of Principle-Based Approach* (April 22 2006)

Available at: <http://www.mortgageintroducer.com/mortgages/10180/135/News_in_depth/-Law_Society> (quoting letter from Margaret Chamberlain, Chairman of the City of London Law Society Regulatory Committee, to John Tiner, Chief Executive of the Financial Services Authority) [Accessed 1/6/13]

Moshiro *Licensing in the Era of Liberalization and Convergence*

Moshiro S *Licensing in the Era of Liberalization and Convergence: The Case Study of the Federal Republic of Nigeria* (2004)

Available at <http://www.itu.int/ITU-D/treg/Case_Studies/Licensing/NIGERIA_CS.pdf> [Accessed 13/3/13]

MRA *Code of Conduct Bureau Declines to Release Assets Declarations by Public Officers*

MRA *Code of Conduct Bureau Declines to Release Assets Declarations by Public Officers* (1999)

Available at <http://mediarightsagenda.net/code-of-conduct-bureau-declines-to-release-assets-declarations-by-public-officers/>; <http://mediarightsagenda.net/court-dismiss-mras-suit-over-public-officers-assets-declarations/> [Accessed 16/7/12]

MRA *Campaigning for Access to Information*

MRA *Campaigning for Access to Information: A Report of the Advocacy for the Freedom of Information Bill* (2003)

Available at <http://mediarightsagenda.net/campaigning-for-access-to-information-in-nigeria-a-report-of-the-legislative-advocacy-programme-for-the-enactment-of-a-freedom-of-information-act/> [Accessed 15/4/13]

N

Nash January 15, 1996 *The New York Times*

Nash N "Holding Compuserve Responsible" January 15, 1996 *The New York Times*

Available at <http://www.nytimes.com/1996/01/15/business/holding-compuserve-responsible.html> [Accessed 20/4/13]

National Assembly of Nigeria Draft Bill *The Computer Security and Critical Information Infrastructure Protection Act* 2005

Available at <http://www.nassnig.org/nass/legislation.php?id=103> [Accessed 3/313]

National Assembly website

Available at <http://www.nassnig.org/nass/legislation.php> [Accessed 25/5/13]

National Population Commission of Nigeria website

Available at <http://www.population.gov.ng> [Accessed 23/11/11]

NIAC (Singapore) *Report on a Model Data Protection Code*

National Internet Advisory Committee (Singapore) *Report on a Model Data Protection Code for the Private Sector*

Available at <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012665-.pdf> [Accessed 30/5/13]

National Outsourcing Policy and Institutional Framework for Nigeria 2007

Available at <http://www.nitda.gov.ng/index.php/legal-and-regulatory/outsourcing-policy> [Accessed 25/5/13]

National Planning Commission *Nigeria Vision 20:2020* (2009)

Available at <http://www.npc.gov.ng/home/doc.aspx?mCatID=68253> [25/5/13]

NCC *Draft Lawful Interception of Communications Regulations*

Available at: <http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=-66&Itemid=8> [Accessed 15/4/13]

NCC *Headlines*

Available at <http://www.ncc.gov.ng/Archive/nccpenaliseglobacom.htm> [Accessed 13/3/13]

NCC *Monthly Subscriber Data*

NCC *Monthly Subscriber Data (September 2010 – August 2011)*

Available at: <http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=-66&Itemid=8>[Accessed 22/10/11]

NCC *Operator Quarterly Summary*

NCC *Operator Quarterly Summary Q3 2010-Q2 2011*

Available at <http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=-65&Itemid=67> [Accessed 22/10/11]

NCC *Quarterly Summary of Operator Data*

NCC *Quarterly Summary of Operator Data September 2010 – June 2011*

Available at < http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=-66&Itemid=8> [Accessed 13/4/13]

NCC Report *Trends in Telecommunications Markets*

NCC Report *Trends in Telecommunications Markets in Nigeria, 2003/2004* (2005)

Available at: <http://www.ncc.gov.ng/Archive/industrystatistics/Trends%20in%20Telecommunications%20Markets%20in%20Nigeria%202004.pdf > [Accessed 4/5/13]

NCC *Sim Registration*

Available at<http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=122-&Itemid=113/> [Accessed 3/3/13]

NCC *Telecommunications Networks Interconnection Regulations* 2003

Available at: <http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=-66&Itemid=8> [Accessed 4/5/13]

NCC website

Available at http://www.ncc.gov.ng/ [Accessed 26/5/13]

Ndukwe *Challenge of Globalisation*

Ndukwe E C A *The Challenge of Globalisation and the Imperative of Creating Adequate ICT Infrastructure in Nigeria* (Paper presented at E-Nigeria 2003 International Conference on Information and Communication Technologies (ICT), Abuja, 10-12 March 2003)

Available at <http://www.ncc.gov.ng/archive/speeches_presentations/EVC's%20Presentation/challenge_of_globalisation_and_imparative_of_creating.pdf> [Accessed on 12/3/13]

Ndukwe *Country Experience in Telecom Market Reforms – Nigeria*

Ndukwe E C A *Country Experience in Telecom Market Reforms* (Presentation by CEO of Nigerian Communications Commission, July 2005)

Available at: <http://www.ncc.gov.ng/archive/speeches_presentations/EVC's%20Presentation/Country%20Experience%20with%20Market%20Reforms%20in%20Telecoms%20%-20%20060705.pdf> [Accessed 4/5/13]

Ndukwe *Evolution of the Telecommunication Industry in Nigeria*

Ndukwe E C A *An Overview of Evolution of the Telecommunication Industry in Nigeria and Challenges Ahead (1999–2003).* A paper presented at the Telecoms Summit, 2003

Available at: <http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=-589:speeches&catid=72:cat-web-speeches&Itemid=93> [Accessed 4/5/13]

Ndukwe *NCC Policy and Strategic Thrust – 2005 and Beyond*

Ndukwe E C A *NCC Policy and Strategic Thrust – 2005 and Beyond* (Presentation at the CEO's Forum by Executive Vice Chairman, Nigerian Communications Commission, 2004)

Available at<http://ncc.gov.ng/archive/3rdntspapers&Communique.htm> [Accessed 13/3/13]

Ndukwe *Nigerian Telecommunications Environment*

Ndukwe E C A *An Overview of the Nigerian Telecommunications Environment* (Presentation by the CEO, Nigerian Communications Commission at the ITU Telecom Africa Conference, 2004)

Available at: <http://www.ncc.gov.ng/archive/speeches_presentations/EVC's%20Presentation/NCC%20CEO%20Presentation%20on%20Overview%20of%20Nigerian%20Telecoms%20Industry.pdf> [Accessed 25/4/13]

Ndukwe *Telecom Liberalisation in Nigeria*

Ndukwe E C A *Telecom Liberalisation in Nigeria* (Paper presented at SATCOM 2005)

Available at <http://www.ncc.gov.ng/archive/speeches_presentations/EVC's%20Presentation/Telecoms%20Liberalisation%20in%20Nigeria.pdf>. [Accessed 12/3/13]

Ndukwe *Telecommunications in Nigeria: The Next Frontier*

Ndukwe E C A *Telecommunications in Nigeria: The Next Frontier* (Paper presented at an NCC seminar by the CEO of the Nigerian Communications Commission in May 2005 2005)
Available at: <http://www.ncc.gov.ng/archive/speeches_presentations/EVC's%20Presentation/Telecommunications%20in%20Nigeria.pdf>. [Accessed 12/3/13]

Ndukwe *Telecoms Regulatory Environment*

Ndukwe E C A *Telecoms Regulatory Environment: Legislation, Regulation and Licensing*
Available at <http://www.ncc.gov.ng/archive/speeches_presentations/EVC's%20Presentation/TELECOM%20REGULATORY%20ENVIRONMENT-%20Judges%20Workshop%-20240105.pdf > [Accessed 13/3/13]

Newswatch magazine website

Available at <http://www.newswatchngr.com> [Accessed 13/3/13]

Nigerian Bar Association *Communiqué*

Nigerian Bar Association *Communiqué Issued at the end of the 51st Annual General Conference of the NBA* held at Port Harcourt (August 2011)
Available at <http://www.britishnigerialawforum.org/communique-issued-at-the-end-of-the-51st-annual-general-conference-of-the-nigerian-bar-association-nba-held-at-port-harcourt-rivers-state-from-august-21-through-26-2011/ > [Accessed 11/6/13]

Nigerian Communications Commission website

Available at <http://www.ncc.gov.ng/> [Accessed 15/3/13]

Nigerian Financial Intelligence Unit website

Available at <http://www.nfiu.gov.ng/> [Accessed 18/6/12]

Nigerian Population Commission website

Available at <http://www.population.gov.ng/> [Accessed 30/5/13]

Nigeria Postal Services website

Available at <http://www.nipost.gov.ng/> [Accessed 5/4/13]

Nigeria Vision 20:2020

Available at: <http://www.npc.gov.ng/home/doc.aspx?mCatID=68253> [Accessed 30/5/13]

NIMC website

National Identity Management Commission website
Available at <http://www.nimc.gov.ng/reports/personal_info_bill.pdf> [Accessed 25/5/13]

NITDA *History of NITDA*

National Information Technology Development Agency *History of NITDA*
Available at <http://www.nitda.gov.ng/index.php/about-nitda/nitda-history> [Accessed 13/3/13]

NITDA *National Policy for Information Technology*

NITDA *The Nigerian National Information Technology Policy* (2001)
Available at <http://www.nitda.gov.ng/docs/policy/ngitpolicy.pdf> [Accessed 13/3/13]

Nwachukwu "Development of Information Technology in Nigeria"

Nwachukwu M A "Development of Information Technology in Nigeria" in Drew E P and Foster F G (ed) *Information Technology in selected Countries: Reports from Ireland, Ethiopia, Nigeria, and Tanzania* (United Nations University Press, 1994)
Available online at: <http://archive.unu.edu/unupress/unupbooks/uu19ie/uu19ie00.htm> [Accessed 4/5/13]

O

Ogg "Toasting the birthday of the integrated circuit"

Ogg E "Toasting the birthday of the integrated circuit" CNET News (9 May 2009)
Available at <<http://news.cnet.com/8301-11386_3-10237155-76.html> [Accessed 23/4/13]

Odinkalu *Nigeria's Freedom of Information Law: How Friends Launched a Movement*

Odinkalu C *Nigeria's Freedom of Information Law: How Friends Launched a Movement* (2011)
Available at <http://www.opensocietyfoundations.org/voices/nigeria-s-freedom-information-law-how-friends-launched-movement> [Accessed 5/3/13]

Okome *State and Civil Society in Nigeria*

Okome M State and Civil Society in Nigeria in the Era of Structural Adjustment Program, 1986-93

Available at: <http://www.africaknowledgeproject.org/index.php/war/article/view/395> [Accessed 10/3/13]

OPSI (UK) website

Office of Public Sector Information (UK) website

Available at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1> [Accessed 30/5/13]

Ovia "Internet Banking: Practices and Potentials in Nigeria"

Ovia J "Internet Banking: Practices and Potentials in Nigeria"

Available at <http://www.zenithbank.com/internet_practices.pdf> [Accessed 4/5/13]

Oyejide and Bankole *Liberalisation of the Services Sector in Nigeria*

Oyejide and Bankole *Liberalisation of the Services Sector in Nigeria: Implications of Unilateral and Multilateral Approaches* (2001)

Available at <http://siteresources.worldbank.org/INTRANETTRADE/Resources/Services-Nigeria.pdf> [24/5/13]

P

Pai and Basu *Offshore Outsourcing*

Pai A K and Basu S *Offshore Outsourcing: Weighing the Risks of Data Protection and Security* (2005) 20th Annual BILETA Queen's University Belfast (2005)

Available at <http://works.bepress.com/subhajitbasu/27> [Accessed 10/4/13]

Panos Institute *The Internet and Poverty: Real help or real hype?*

Panos Institute *The Internet and Poverty: Real help or real hype?* (1998) Panos Briefing No 28
Available at: <http://dspace.cigilibrary.org/jspui/bitstream/123456789/14487/1/The%20-Internet%20and%20Poverty%20Real%20Help%20or%20Real%20Hype.pdf?> [Accessed 15/7/12]

Pavli *Is Europe's Top Court Finally Embracing Right to Know?*

Pavli D *Is Europe's Top Court Finally Embracing Right to Know?* (2012)
Available at: < http://www.opensocietyfoundations.org/voices/case-watch-europe-s-top-court-finally-embracing-right-know> [Accessed 8/4/13]

Perrolle *Computers and Social Change*

Perrolle J A *Computers and Social Change* 1.1.1.1. (1999)
Available at <http://www.ccs.neu.edu/home/perrolle/book/chapter1.html> [Accessed 5/3/13]

Perritt "Regulatory Models for Protecting Privacy"

Perritt H H "Regulatory Models for Protecting Privacy in the Internet" chp 3 in *Privacy and Self-Regulation in The Information Age* (NTIA) (1997)
Available at <http://www.ntia.doc.gov/page/chapter-3-models-self-regulation> [Accessed 30/5/13]

Polity.org.za website

Available at http://www.polity.org.za [Accessed 3/1/14]

Pontin *New economy does not mean laws of economics have overturned*

Pontin J *New economy does not mean laws of economics have overturned* (3 October 2000)
Available at: <http://www.ephrem.org/dehai_news_archive/2000/oct00/0016.html> [Accessed 4/5/13]

Prichard and Mulligan *The Poverty of Sovereignty*

Prichard A and Mulligan M *The Poverty of Sovereignty*

Available at <http://turin.sgir.eu/uploads/Mulligan-the_poverty_of_sovereignty.pdf> [Accessed 14/05/08]

Privacilla.org website

Available at <http://www.privacilla.org/government/cmppa.html> [Accessed 30/5/13]

Privacilla *Privacy and Government*

Available at <http://www.privacilla.org/government/cmppa.html> [Accessed 30/5/13]

Privacy Rights Clearinghouse *Chronology of Data Breaches*

Privacy Rights Clearinghouse *A Chronology of Data Breaches Reported since the ChoicePoint Incident*

Available at <http://www.privacyrights.org/data-breach> [Accessed 20/3/13]

Privacy Rights Clearinghouse *Identity Theft and Data Breaches*

Privacy Rights Clearinghouse *Identity Theft and Data Breaches*

Available at https://www.privacyrights.org/Identity-Theft-Data-Breaches> [Accessed 23/11/07]

Privacy Protection Study Commission *Personal Privacy in an Information Society*

Privacy Protection Study Commission *The Report of The Privacy Protection Study Commission: Personal Privacy in an Information Society* (1977)

Available at <http://epic.org/privacy/ppsc1977report/> [Accessed 15/4/13]

Privacy Protection Study Commission "Technology and Privacy"

Privacy Protection Study Commission (USA) "Technology and Privacy" Appendix 5 in *The Report of The Privacy Protection Study Commission: Personal Privacy in an Information* Society (1977)

Available at <http://www.epic.org/privacy/ppsc1977report> [Accessed 15/4/13]

Pyramid Research *The Impact of Mobile Services in Nigeria*

Pyramid Research *The Impact of Mobile Services in Nigeria: How Mobile Technologies are Transforming Economic and Social Activities* (2010)

Available at <http://www.pyramidresearch.com/documents/IMPACTofMobileServicesIn-NIGERIA.pdf> [Accessed 23/12/12]

Punch newspaper website

Available at <http://www.punchng.com> [Accessed 13/3/13]

R

Raab et al *Adequacy of the Level of Protection of Individuals*

Raab C D, Bennett C J, Gellman R M and Waters N *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer* (European Commission Tender No XV/97/18/D) 202 (1998)

Available at <http://www.colinbennett.ca/Recent%20publications/adequat_en.pdf.> [Accessed 30/5/13]

Rich and Harris *Predictive Analytics*

Rich D and Harris J G *Why Predictive Analytics Is A Game-Changer* (2010)

Available at <http://www.forbes.com/2010/04/01/analytics-best-buy-technology-data-companies-10-accenture.html> [Accessed 13/4/13]

Right2info *List of Countries with Actionable ATI Laws*

Right2info.org *List of Countries with Actionable ATI Laws* (2012)

Available at <http://www.right2info.org/recent/100-countries-with-ati-provisions> [Accessed 17/7/12]

Right2info *Access to information laws: overview and statutory goals*

Right2info.org *Access to information laws: overview and statutory goals*

Available at <http://www.right2info.org/access-to-information-laws> [Accessed 16/1/14]

Rowland 1997 (5) *Web JCLI*

Rowland D "The EC Database Directive: An Original Solution to an Unoriginal Problem?" 1997 (5) *Web Journal of Current Legal Issues*

Available at <http://webjcli.ncl.ac.uk/1997/issue5/rowland5.html> [Accessed 4/3/13]

S

Safier *Between Big Brother and the Bottom Line*

Safier S *Between Big Brother and the Bottom Line: Privacy in Cyberspace*

Available at <http://www.vjolt.net/vol5/issue2/v5i2a6-Safier.html> [Accessed 24/5/13]

Salbu *The EU Data Privacy Directive*

Salbu S R "The European Union Data Privacy Directive and International Relations" *William Davidson Working Paper* No 418 (2001)

Available at <wdi.umich.edu/files/publications/workingpapers/wp418.pdf> [Accessed 22/5/13]

Samuelson and Varian *The "New Economy"*

Samuelson P and Varian H *The "New Economy" and Information Technology Policy* (2001) Available at <www.sims.berkeley.edu/~hal/Papers/infopolicy.pdf> [Accessed 5/3/13]

Savage and Risen 31st March 2010 *New York Times*

Savage C and Risen J "Federal Judge Finds N.S.A. Wiretaps Were Illegal" *New York Times* (31 March 2010)

Available at <http://www.nytimes.com/2010/04/01/us/01nsa.html> [Accessed 13/3/13]

Scott *Standard-Setting in Regulatory Regimes*

Scott C *Standard-Setting in Regulatory Regimes* UCD Working Papers in Law, Criminology & Socio-Legal Studies (Research Paper No 07/2009)

Available at <http://ssrn.com/abstract=1393647> [Accessed 23/5/13]

Singleton *Privacy as a Trade Issue*

Singleton S *Privacy as a Trade Issue: Guidelines for U.S. Trade Negotiators* (2002) Available at <http://cei.org/studies-issue-analysis/privacy-trade-issue-guidelines-us-trade-negotiators> [Accessed 3/3/13]

Smith *Protecting Consumers and the Marketplace*

Smith B *Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation* (2005)
Available at <http://www.netcaucus.org/speakers/2005/smith/privacyspeech.pdf> [Accessed 26/5/13]

Srivastava *Issues in Institutional Design of Regulatory Agencies*

Srivastava L *Issues in Institutional Design of Regulatory Agencies*
Available at <http://www.teriin.org/upfiles//pub/papers/ft23.pdf > [Accessed 3/6/13]

Standard Chartered Bank Plc website

Available at <http://www.standardchartered.com/ng/data-protection-privacy-policy/en/> [Accessed 25/5/13]

Stewart *International Transfers of Personal Data*

Stewart B *International Transfers of Personal Data: Candidate for Adequacy - The New Zealand Case* (Notes for an address to the Privacy Laws & Business 14th Annual Conference, St John's College, Cambridge) (2001)
Available at <http://privacy.org.nz/international-transfers-of-personal-data-candidate-for-adequacy-the-new-zealand-case/> [Accessed 30/5/13]

Stewart *The Economics of Data Privacy*

Stewart B *The Economics of Data Privacy: Should We Place a Dollar Value on Personal Autonomy and Dignity?*
Available at <26konferencja.giodo.gov.pl/data/resources/StewartB_paper.pdf> [Accessed 10/3/13]

Stoddart *Privacy in the Marketplace*

Stoddart J *Privacy in the Marketplace* Remarks of the Privacy Commissioner of Canada at the Canadian Marketing Association Regulatory Affairs Conference (14 September 2006)

Available at <http://www.privcom.gc.ca/speech/2006/sp-d_060914_e.asp> [Accessed 10/4/13]

Swire "Markets, Self-Regulation and Government Enforcement"

Swire P "Markets, Self-Regulation and Government Enforcement in Protection of Personal Information" in *Privacy and Self-Regulation in the Information Age* (NTIA) (1997)

Available at <http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy> [Accessed 30/5/13]

T

Thisday newspaper website

Available at <http://www.thisdaylive.com> [Accessed 13/3/13]

The Independent newspaper "Number of Internet users worldwide reaches two billion: UN" 26 January 2011

Available at <http://www.independent.co.uk/life-style/gadgets-and-tech/number-of-internet-users-worldwide-reaches-two-billion-un-2195157.html> [Accessed 23/5/13]

Thorson and Sedore *Spam and Personal Data Privacy*

Thorson S J and Sedore C M *Spam and Personal Data Privacy* (2002)

Available at <http://www.academia.edu/294058/SPAM_AND_PERSONAL_DATA_-PRIVACY> [Accessed 20/4/13]

Transparency International (TI) *Corruption Perception Index*

Transparency International (TI) *Corruption Perception Index* (2006)

Available at <http://archive.transparency.org/policy_research/surveys_indices/cpi/2006> [Accessed 3/3/13]

Tuckness "Locke's Political Philosophy"

Tuckness A "Locke's Political Philosophy" in Zalta E N (ed) *The Stanford Encyclopedia of Philosophy* (2005)

Available at <http://plato.stanford.edu/archives/win2005/entries/locke-political/> [Accessed 30/3/13]

Turn *An Overview of Transborder Data Flow Issues*

Turn R *An Overview of Transborder Data Flow Issues*. sp, pp.0003, 1980 IEEE Symposium on Security and Privacy, (1980)

Available at <http://doi.ieeecomputersociety.org/ 10.1109/SP.1980.10010>. [Accessed 19/4/13]

U

UK Parliament *Fraud and Computer Data Matching*

UK Parliament *Fraud and Computer Data Matching* (Post note 93 Feb 1997)

Available at <http://www.parliament.uk/Templates/BriefingPapers/Pages/BPPdfDownload.-aspx?bp-id=POST-PN-93> Accessed [20/4/13]

UNESCO Institute for Statistics *Education (all levels) profile – Nigeria*

Available at <http://www.uis.unesco.org/searchcenter/Pages/Results.aspx?k=EDUCATION-%20PROFILE%20NIGERIA&s=UIS_Site_EN> [Accessed 23/5/13]

USAID Website

United States Agency for International Development Website

Available at <http://www.usaid.gov/> [Accessed 10/3/13]

US Census Bureau Website

Available at <http://www.census.gov/popclock/> [Accessed 25/5/13]

US State Department *Annual Human Rights Report 2005 on Nigeria*

Available at <http://www.state.gov/g/drl/rls/hrrpt/2005/61586.htm> [Accessed 4/4/13]

US State Department *Human Rights Report 2010*

Available at: <http://www.state.gov/j/drl/rls/hrrpt/2010/af/154363.htm> [Accessed 5/4/13]

US Department of Commerce, International Trade Administration website

Available at <http://trade.gov/publications/> [Accessed 23/11/11]

US Department of Justice *Identity Theft and Identity Fraud*

Available at <http://www.usdoj.gov/criminal/fraud/websites/idtheft.html> [Accessed 25/5/13]

US Department of Commerce, International Trade Administration *Telecomm Market Summary: China*

Available at: <http://web.ita.doc.gov/ITI/itiHome.nsf/9b2cb14bda00318585256cc40068ca-69/7a19947d610987658525788c0041ea3d/$FILE/telecom%20market%20snapshot-china.-pdf> [Accessed 13/4/13]

US-EU & US-Swiss *Safe Harbor Frameworks*

Available at <http://export.gov/safeharbor/index.asp> [Accessed 5/4/13]

US Library of Congress *Country Studies*

Available at <http://memory.loc.gov/frd/cs/ngtoc.html> [Accessed 10/3/13]

US Library of Congress (Thomas) website

Available at <http://thomas.loc.gov/home/bills_res.html> [Accessed 20/3/13]

V

Van Der Linden and Hengeveld *Critical Success Factors for Obtaining Outsourcing Projects*

Van Der Linden B and Hengeveld S *Critical Success Factors for obtaining outsourcing projects for Uganda*

Available at: <http://www.bartvanderlinden.eu/mediapool/74/746182/data/Critical_-Success_Factors_for_obtaining_outsourcing_projects_for_Uganda_final.pdf>. [Accessed 10/4/13]

Vanguard newspaper website

Available at <http://www.vanguardngr.com> [Accessed 13/3/13]

W

Wallison *Fad or Reform*

Wallison P J *Fad or Reform: Can Principles-Based Regulation Work in the United States?* (American Enterprise Institute for Public Policy Research) (2007)

Available at <http://www.aei.org/article/economics/financial-services/fad-or-reform/>. [Accessed 2/6/13]

Wilson *Globalization, Information Technology, and Conflict*

Wilson III E J *Globalization, Information Technology, and Conflict in the Second and Third Worlds: A Critical Review of the Literature* (1998)

Available at http://www.rbf.org/sites/default/files/Globalization,_Information_Technology,_-and_Conflict.pdf>. [Accessed 4/5/13]

WSIS Documents

Available at <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160> [Accessed 20/4/13]

Wolf and Tobin "Extraterritorial Applicability of US Privacy Laws"

Wolf C and Tobin T P "Extraterritorial Applicability of US Privacy Laws" Chp 28 *in* Proskauer's *E-Guide on International Litigation and Arbitration: Managing, Resolving and Avoiding Cross-Border Business or Regulatory Disputes* (2007)

Available at: <http://www.proskauerguide.com/toc> [Accessed 13/6/12]

Wood *Statute of the International Law Commission*

Wood M *Introduction to the Statute of the International Law Commission*

Available at <http://untreaty.un.org/cod/avl/ha/silc/silc.html> [Accessed 21/5/13]

World Bank *World Development Indicators*

World Bank *World Development Indicators Database*
Available at: <http://databank.worldbank.org/data/views/variableselection/selectvariables.-aspx?source=world-development-indicators>. [Accessed 10/3/13]

World Economic Forum *Global Information Technology Report* (2012)

Available at <http://www.weforum.org/reports/global-information-technology-report-2012> [Accessed 3/3/13]

World Trade Organisation General Agreement on Trade in Services (GATS) website

Available at: <http://www.wto.org/english/docs_e/legal_e/legal_e.gtml#services> [Accessed 15/6/08]

White *People, Not Places*

White J C *People, Not Places: A Policy Framework for Analyzing Location Privacy Issues* (2003)
Available at <http://epic.org/privacy/location/jwhitelocationprivacy.pdf> [Accessed 13/3/13]

Z

Zakon *Hobbes Internet Timeline* 10.2

Zakon R H *Hobbes Internet Timeline* 10.2 (1993-2011)

Available at <http://www.zakon.org/robert/internet/timeline//> [Accessed 8/3/13]

Zenith Bank *Privacy Policy*

Available at <http://www.zenithbank.com/privacy.cfm> [Accessed 20/3/13]

DOCUMENTS ISSUED BY INTERNATIONAL ORGANISATIONS, DATA PROTECTION AGENCIES/COMMISSIONERS, CONVENTIONS, DIRECTIVES, REPORTS, ETC

International Organisations

African Union

African Charter on Human and Peoples Rights (1981) OAU Doc CAB/LEG/67/3 rev 5, 21 ILM 58 (1982)

African Charter on the Rights and Welfare of the Child (1990). OAU Doc. CAB/LEG/24.9/49 (1990)

OAU *Convention on the Prevention and Combating of Terrorism* (1999)

APEC

The APEC *Privacy Framework* (APEC, 2005).

Commonwealth

Commonwealth Human Rights Initiative Report (CHRI) *Looking for the Right to Information in the Commonwealth* (2003)

Commonwealth Organisation (Heads of Government) *Principles and Guidelines on the Right to Know* (1999)

Council of Europe

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 Individuals with Regard to Automatic Processing of Personal Data* (CETS No 108) (1981)

Council of Europe *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 CETS No 181* (2001)

Council of Europe Committee of Ministers, 1031st meeting (2 July 2008), Decision Item 10.2. *Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No108) (T-PD). (Strasbourg, 13-14 March 2008)

Council of Europe *Convention on Cybercrime* (CETS 185) (8 November 2001)

Council of Europe *European Convention on Human Rights* (as amended by Protocols Nos. 11 and 14) (CETS 5). (4th November 1950)

Data Protection Agencies/Commissioners

Data Protection and Privacy Commissioners Resolution on the Urgent Need for Protecting Privacy in a Borderless World and for reaching a Joint Proposal for setting International Standards on Privacy and Data Protection (30th International Conference of Data Protection and Privacy Commissioners, 2008)

Data Protection and Privacy Commissioners Conference *Montreux Declaration on the Protection of Personal Data in a Globalised World: A Universal Right Respecting Diversity* (2005)

Information Commissioner's Office (UK) *What Price Privacy? The Unlawful Trade in Confidential Personal Information* (2006)

Information Commissioner's Office (UK) *Privacy and Electronic Communications Regulations* (2003)

Information Commissioner's Office (UK) *Data Protection Regulatory Action Policy* (2004)

Privacy Commissioner of Canada *Annual Report to Parliament 2006-2007: Report on the Privacy Act* (Office of the Privacy Commissioner of Canada, 2007)

Ecowas

ECOWAS *Treaty of the Economic Community of West African States* (1975); See also Revised Treaty of the Economic Community of West African States (1993)

ECOWAS *Supplementary Act on Personal Data Protection within ECOWAS* A/SA (2010)

European Union / European Commission

European Commission *Decisions on the adequacy of the protection of personal data in third countries.*

Available at <http://ec.europa.eu/justice/data-protection/document/international-transfers/-adequacy/index_en.htm> [Accessed 25/5/13]

European Commission *Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on t*he *Adequate Protection of Personal Data provided in Switzerland* 2000/519/EC, Official Journal L 215 (2000)

European Commission *Decision pursuant to Directive 95/46/EC on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries* 2001/497/EC, Official Journal L 181 (2001)

European Commission *Explanatory Memorandum on the Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* COM (2012) 10 (2012)

European Commission *Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications of Regulation: Towards an Information Society Approach* COM (97) 623 final, 3 (1997)

European Commission *Press Release EU approves New Zealand's data protection standards in step to boost trade.* Available at <http://europa.eu/rapid/press-release_IP-12-1403_en.pdf> [Accessed 30/5/13]

European Commission *Proposal for a Council Framework Decision on Attacks against Information Systems* 2002/C 203 E/16 Official Journal C 203 E (2002)

European Commission *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* COM (2012) 11 final (Jan. 15, 2012)

European Commission *Report on Europe and the Global Information Society: Recommendations of the High-level Group on the Information Society to the Corfu European Council. Bulletin of the European Union,* (*Bangemann Report*) Supplement No. 2/94 (1994)

European Commission Working Party on the Protection of Individuals with Regard to the Processing of Personal Data *First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy* (DG XV D/5020/97 WP4) (1997)

European Commission Working Party on the Protection of Individuals with Regard to the Processing of Personal Data *Judging Industry Self-Regulation: When does it make a meaningful contribution to the level of data protection in a third country?* (DG XV D/5057/97 WP7) (1998)

European Commission Working Party on the Protection of Individuals with Regard to the Processing of Personal Data *Opinion 1/2008 o*n *Data Protection Issues Related to Search Engines* (00737/EN WP 148) (2008)

European Commission Working Party on the Protection of Individuals with Regard to the Processing of Personal Data *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000* (5095/00/EN/Final WP40) (2001)

European Commission Working Party on the Protection of Individuals with Regard to the Processing of Personal Data *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (DG XV D/5025/98 WP12) (1998)

European Commission Working Party on the Protection of Individuals with Regard to the Processing of Personal Data *Working Document on the Applicable Law in case of Personal Data Processing by non-EU Web Sites* (5035/01/EN/Final WP 56) (2002)

European Union *Charter of Fundamental Rights* Official Journal of the European Communities C 364/1 (2000)

European Union *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* Official Journal L 281 (1995)

European Union *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996, on the legal protection of databases* Official Journal L 77/20 (1996)

European Union *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 (Directive on privacy and electronic communications)* Official Journal L 201/37 (2002)

European Union *Directive 2006/24/EC of the European Parliament and of the Council 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* Official Journal L 105, 13.4 (2006)

European Union *Regulation (EC) 45/2001 of the European Parliament and of the Council of 18th 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* Official Journal L 008 (2001)

European Union *Trade with the World and EU Trade with Nigeria* (2012)
Available at <http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_113427.pdf> [Accessed 10/4/13]

European Union *Treaty Establishing the European Community* Official Journal C 321E (2006)

ITU

ITU International Telecommunication Convention (ITU, 1982)

ITU *Licensing in the Era of Liberalization and Convergence: The Case Study of the Federal Republic of Nigeria* (ITU, 2004)

ITU *Survey on Anti-Spam Legislation Worldwide* (Doc No CYB/06) (ITU, 2005)

ITU *The World in 2010: ICT Facts and Figures* (ITU, 2010)

Law Reform Commissions' Reports

Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)* Executive Summary (2008)

Australian Law Reform Commission *Privacy Report* Vol 1 No 22 (1983)

Law Reform Commission of Hong Kong *Consultation Paper on Civil Liability for Invasion of Privacy* (LRCHK, 1999)

Law Reform Commission of Hong Kong (Privacy Sub-committee) *Reform of the Law Relating to Information Privacy: A Consultative Document* (LRCHK, 1993)

Law Reform Commission of Ireland Report *Surveillance and the Interception of Communications* (1998).

Law Reform Commission of South Africa *Privacy and Data Protection* (Discussion Paper 109 Project 124) (SALRC, 2005)

OECD

OECD *Consumer Protection Guidelines for E-Commerce* (OECD, 1999)

OECD *Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data* (OECD, 1980)

OECD *Guidelines for Consumer Protection in the Context of Electronic Commerce* (OECD, 1999)

OECD *Global Information Infrastructure-Global Information Society (GII-GIS): Policy Requirements* (OECD, 1997)

OECD *Recommendation of the Council of the Organisation for Economic Cooperation and Development concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 1980)

OECD *Regulatory Reform and International Standardisation* (OECD Working Party of the Trade Committee) (OECD, 1999)

OECD *Report Growth in Services: Fostering Employment, Productivity and Innovation* (OECD, 2005)

OECD *Report on the Cross-border Enforcement of Privacy Laws* (OECD, 2006)

UN

UNCTAD *E-Commerce and Development Report* (UNCTAD, 2003)

UNCTAD *Digital Divide: ICT Development Indices 2004* (UNCTAD, 2005)

UNCTAD *Tradability of Consulting Services and its Implications for Developing Countries* (UNCTAD, 2002)

UN Centre on Transnational Corporations *Transnational Corporations and Trans-border Data Flows: A Technical Paper* 46. (UN, 1982)

UN Centre on Transnational Corporations *Transnational Corporations and Transborder Data Flows: Background and Overview* (Elsevier, 1984)

UN Department of Economic and Social Affairs/Population Division *World Population Prospects: The 2012 Revision, Volume I: Comprehensive Tables.* Available at <United Nations Department of Economic and Social Affairs/Population Division World Population Prospects: The 2012 Revision, Volume I: Comprehensive Tables.>. [Accessed 10/3/13]

UN Department of Economic and Social Affairs/Population Division *World Population Prospects: The 2012 Revision, Volume I: Comprehensive Tables* (UN, 2012)

UNDP *Human Development Report 2001: Making New Technologies work for Human Development* (UN, 2001)

UNDP *Human Development Report 2004* (UNDP, 2004)

UNDP *National Human Development Report* (UNDP, 1998)

UN Economic and Social Commission for Asia and the Pacific *Good Practices in Information and Communication Technology Policies in Asia and the Pacific* (ST/ESCAP/2347) (United Nations, New York, 2004) 56

UN General Assembly *Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families* Doc. A/RES/45/158 (1990)

UN General Assembly *Convention on the Rights of the Child* (UN, 1989)

UN General Assembly *Convention against Transnational Organised Crime*; Resolution /55/25 of the (UN, 2000)

UN General Assembly *International Covenant on Civil and Political Rights* (*Resolution 2200A (XXI))* (UN, 1966)

UN General Assembly Resolution 174 (II) of 21 November 1947 (Establishment of the International Law Commission) (UN, 19470

UN General Assembly Resolution 59(1), 65th Plenary Meeting 14 December (UN, 1946)

UN General Assembly Resolution 45/95, UN Doc A/RES/45/95, 14 December (UN, 1990)

UN General Assembly *Report of the International Law Commission* (58th Session) (Annex D) Supplement No. 10 (A/61/10) (UN, 2006)

UN General Assembly *Statute of the International Law Commission* (UN, 1947)

UN General Assembly *Universal Declaration of Human Rights* (Resolution 217A (III)) (UN, 1948)

UN *Global E-government Readiness Report 2005: From E-government to E-inclusion* (UN, 2005)

UN *Guidelines for the Regulation of Computerized Personnel Data Files* (1990) UN Doc E/CN4/1990/72

UNESCO Institute for Statistics *Education (all levels) profile – Nigeria.* Available at < http://www.uis.unesco.org/searchcenter/Pages/Results.aspx?k=EDUCATION%20PROFILE%20NIGERIA&s=UIS_Site_EN>. [Accessed 23/5/13

UNESCO *World Communication Report: The Media and the Challenges of the New Technologies* (UNESCO, 1997)

UNIDO *Enabling Developing Countries to Participate in International Trade: Strengthening the Supply Capacity* (UNIDO, 2002)

UN Office on Drugs and Crime (UNODC) *A Review of the Legal Regime against Terrorism in West and Central Africa* (UN, 2008)

UN *Points for Possible Inclusion in Draft International Standards Concerning Respect for the Privacy of the Individual in the light of Modern Recording and Other Devices* (UN *Doc E/CN.4/1116* (1976)

UN *Points for Possible Inclusion in Draft International Standards for the Protection of the Rights of the Individual against Threats Arising from the Use of Computerised Personal Data Systems* UN Doc *E/CN.4/1233* (1976)

UN Special Rapporteur (Hussain A) *Report on Promotion and Protection of the Right to Freedom of Opinion and Expression* E/CN.4/1998/40 (1998)

UN Special Rapporteur (Hussain A) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* E/CN.4/2000/63 (2000)

WSIS

World Summit on the Information Society (WSIS) *Declaration of Principles and Plan of Action* WSIS-03/GENEVA/DOC/0004 (WSIS, 2003)

WTO

WTO *Agreement on Technical Barriers to Trade, Annex 1A to the Marrakesh Agreement Establishing the World Trade Organization* (1994)

WTO General Council *Work Programme on Electronic Commerce* WT/L/274 (WTO, 1998)

WTO GATT 1994: General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations 17 (1999), 1867 U.N.T.S. 187, 33 I.L.M. 1153 (WTO, 1994)

WTO GATS: General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations 284 (1999), 1869 U.N.T.S. 183, 33 I.L.M. 1167 (WTO, 1994)

WTO General Council *Work Programme on Electronic Commerce* WT/L/274 (WTO, 1998)

WTO *Nigeria: Schedule of Specific Commitments (GATS/SC/65/Suppl.1)*. Available at: <http://www.esf.be/pdfs/GATS%20UR%20Commitments/Nigeria%20SoC%20Supplement%201.pd>. [Accessed 25/5/13]

WTO *World Trade Report: Exploring the links between trade, standards and the WTO* (WTO, 2005)

OTHERS

Inter-American Commission on Human Rights *American Convention on Human Rights* (ACHR, 1969)

Privacy International *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Development* (Privacy International, 2002)

NEWSPAPERS, MAGAZINES (PRINT AND INTERNET-BASED), DICTIONARIES AND ENCYCLOPAEDIAS

A

Abayomi 12th June 2010 *Daily Independent*

Abayomi A "Nigeria: NCC and GSM Tariff Slash" *Daily Independent* newspaper (12 June 2010) Available at <http://allafrica.com/stories/201006140468.html> [Accessed 13/3/2013]

Adaramola 26 October 2011 *Daily Trust*

Adaramola Z "Quality of Service - NCC Issues Deadline to MTN, GLO, Airtel" *Daily Trust* (26 October 2011)

Ademiluyi 11 December 2000 *TELL* (magazine) 52

Ademiluyi S "Plastic Money is it" *TELL* (magazine) (11th December 2000) 52-53

Agre "Personal Information in the Digital Age"

Agre P E "Personal Information in the Digital Age" in *Encarta Yearbook* CD-ROM (Microsoft, 1998)

Ahiuma-Young 5 August 2010 *Vanguard*

Ahiuma-Young V "Nigeria Internet users hit 43.9m" *Vanguard* newspaper (5 August 2010) Available at <http://www.vanguardngr.com/2010/08/nigeria-internet-users-hit-43-9m/> [Accessed 4/5/13]

Ajakaye 16 Nov 2005 *Thisday*

Ajakaye T "Telecom Summit Advocates Merger of NBC, NCC, NITDA" *Thisday* newspaper (16 November 2005)
Available at <http://allafrica.com/stories/200511170263.html> [Accessed 13/3/13]

Anaba 26 June 2012 *Vanguard*

Anaba I "Release your salary details, court orders NASS" in *Vanguard* newspaper 26th June 2012. Available at <http://www.vanguardngr.com/2012/06/release-your-salary-details-court-orders-nass/>. [Accessed 20/7/12]

Angwin 30 July 2010 *The Wall Street Journal*

Angwin J "The Web's New Gold Mine: Your Secrets" *The Wall Street Journal* newspaper (Europe edition) (30 July 2010)
Available at: <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html> [Accessed 10//13]

Aragba-Akpore 23 November 1999 *The Guardian* 41

Aragba-Akpore S "How Internet can transform banking in the next century" *The Guardian* newspaper (23 November 1999) 41

B

Ball 16 January 2014 *Guardian* (UK)

Ball J "nsa-collects-millions-text-messages-daily-untargeted-global-sweep" *Guardian (UK)* newspaper (16 January 2014)
Available at <http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep> [Accessed 16/1/14]

***Businessday* 1 January 2013**

Businessday "4.5% of Nigerians own PC, NBS survey*"* (1 January 2013)
Available at: <http://www.businessdayonline.com/NG/index.php/tech/telecoms/49654-45-of-nigerians-own-pc-nbs-survey> [Accessed 4/5/13]

C

Chandrasekhar, Waldrop and Trotman 23 July 2012 *The Telegraph*

Chandrasekhar I, Waldrop M and Trotman A "Phone Hacking: Timeline of the Scandal" *The Telegraph* newspaper (23 July 2012)
Available at <http://www.telegraph.co.uk/news/uknews/phone-hacking/8634176/Phone-hacking-timeline-of-a-scandal.html> [15/9/12]

D

***Daily Mail Online* 23 June 2005**

Daily Mail Online "Indian call centre staff 'selling bank details'" (23 June 2005) Available at: <http://www.dailymail.co.uk/news/article-353269/Indian-centre-staff-selling-bank-details.html>. [Accessed 20/3/13]

E

Efrati 18 May 2011 *Wall Street Journal* B2

Efrati A "'Like' Button Follows Web Users" *Wall Street Journal* newspaper (May 18 2011) B2. Available at: <http://online.wsj.com/article/SB10001424052748704281504576329-441432995616.html> [Accessed 18/10/12]

***Encyclopaedia Britannica* "Defense Advanced Research Projects Agency (DARPA)" (Encyclopaedia Britannica Student and Home Edition, Chicago 2010)**

***Encyclopaedia Britannica* "Fax" (Encyclopaedia Britannica Student and Home Edition, Chicago 2010)**

***Encyclopaedia Britannica* "Information processing" (Encyclopaedia Britannica Student and Home Edition, Chicago 2010)**

***Encyclopaedia Britannica* "Printing" (Encyclopaedia Britannica Student and Home Edition, Chicago 2010)**

***Encyclopaedia Britannica* "Telegraph" (Encyclopaedia Britannica Student and Home Edition, Chicago 2010)**

***Encyclopædia Britannica* "Spyware" (Encyclopaedia Britannica Student and Home Edition, Chicago 2010)**

Ezigbo 17 October 2005 *Thisday*

Ezigbo O "Nigeria to Earn $8bn on ICT By 2010" *Thisday* newspaper (17th Oct 2005) Available at <http://allafrica.com/stories/200510170944.html> [Accessed 12/8/12]

F

Famakinwa 18 Jan 2001 *Thisday*

Famakinwa S "Nigeria: For Nigeria, It's World-Wide Wait" *Thisday* newspaper (18 January 2001)
Available at <http://allafrica.com/stories/200101180189.html> [Accessed 10/3/13]

G

Giginyu 3 January 2012 *Daily Trust*

Giginyu I M "Glo rewards 11 subscribers" *Daily Trust* newspaper (3 January 2012)
Available at: <http://dailytrust.com.ng/index.php?option=com_content&view=article&id=-151447:glo-rewards-11-subscribers&catid=3:business&Itemid=3> [Accessed 3/1/12]

Gleick 29 September 1996 *The New York Times*

Gleick J "Big Brother is Us" *The New York Times* newspaper (29 September 1996)
Available at <http://www.nytimes.com/1996/09/29/magazine/big-brother-is-us.html?page-wanted=all&src=pm> [Accessed 26/11/13]

H

Heussner 1 March 2011 *ABC News*

Heussner K M "Creepy or Convenient? Apps for Tracking, Keeping Tabs" *ABC News* (1 March 2011)
Available at <http://abcnews.go.com/Technology/smartphone-apps-tracking-keeping-tabs-past-lovers-people/story?id=13022144#.UNxOUmInOvM>. [Accessed 25/10/12]

Ho 12 November 2000 *The Sunday Times* (Singapore) 47

Ho A "Globalisation or globaloney?" *The Sunday Times (Singapore)* newspaper 47 (12 November 2000)

I

Ikoabasi 29 August 2011 *Daily Trust*

Ikoabasi C "Second National Carrier's Emergence and the Growth of Telecoms Technology" *Daily Trust* newspaper (29 August 2011)

Available at <http://www.dailytrust.com.ng/~trust/index.php/it-world/36701-second-national-carriers-emergence-and-the-growth-of-telecoms-technology> [Accessed 13/3/13].

***Independent* 26 January 2011**

Independent "Number of Internet users worldwide reaches two billion: UN" (26 January 2011)

Available at <http://www.independent.co.uk/life-style/gadgets-and-tech/number-of-internet-users-worldwide-reaches-two-billion-un-2195157.html> [Accessed 23/5/13]

L

Lohor, Akunna, and Andoor 13 July 2006 *Thisday*

Lohor J Akunna C and Andoor D "Nigeria: Security Operatives Swoop on Atiku's Bank Records" *Thisday* online newspaper of (13 July 2006)

Available at <http://allafrica.com/stories/200607130115.html> [Accessed 5/4/13]

M

Mandel 30 December 1996 *Businessweek*

Mandel M J "The Triumph of the New Economy" *Businessweek* magazine (30 December 1996)

Available at <http://www.businessweek.com/1996/53/b35081.htm> [Accessed 5/3/13]

***Merriam Webster Dictionary* "Cookies" Encyclopaedia Britannica Student and Home Edition (Chicago 2010)**

***Merriam Webster Dictionary* "Data processing" Encyclopaedia Britannica Student and Home Edition (Chicago 2010)**

Muraina and Nkanga 19 March 2010 *Thisday*

Muraina F and Nkanga E "Court Orders NCC to Restore Mobitel's 2.3ghz Licence" *Thisday* newspaper (19th March 2010)

N

Nkanga 31 March 2011 *Thisday*

Nkanga E "Non-Passage of Cyber Crime Bill Decried" *Thisday* 31st March 2011

Available at <http://www.thisdaylive.com/articles/non-passage-of-cyber-crime-bill-decried/88750/> [Accessed 20/3/13]

Nurudeen 6 January 2012 *Daily Trust*

Nurudeen N A "46.7% Nigerians lack access to telephone services" *Daily Trust* (6 January 2012).

Available at <http://www.dailytrust.com.ng/index.php/business/151766-467-nigerians-lack-access-to-telephone-services>. [Accessed 20/5/12]

Nwankwo 3rd July 2011 *Leadership* newspaper

Nwankwo B "NITEL/Mtel Privatisation: Can BPE Ever Get It Right?" *Leadership* newspaper (3rd July 2011)

Available at http://www.leadership.ng/nga/articles/1398/2011/07/03/nitelmtel_Privatisation_-can_bpe_ever_get_it_right.html>. [Accessed 13/3/13]

Nweke 15th August 2011 *Daily Champion*

Nweke R "Harmonised National ICT Policy Out Soon - Johnson" *Daily Champion* (15 August 2011)

O

Obi 3rd May 2012 *Thisday*

Obi P "Nigeria: When NCC, NESREA Flex Muscles Over Regulatory Issues" *Thisday* newspaper (3 May 2012)

Available at <http://allafrica.com/stories/201205030403.html> [Accessed 28/12/12]

Obi, Udonquak and Majekodumi 7 June 2011 *Businessdayonline*

Obi D, Udonquak A and Majekodunmi I "Jonathan wakes up investigative journalism in Nigerian media" *Businessdayonline* newspaper (7 June 2011)

Available at <http://www.businessdayonline.com/NG/index.php/media-business/22654-jonathan-wakes-up-investigative-journalism-in-nigerian-media-> [Accessed 5/3/13]

Odell 2 August 2005 *Financial Times*

Odell M "Use of Mobile Helped Police Keep Tabs on Suspect and Brother" *Financial Times* newspaper (2 August 2 2005)
Available at <http://www.ft.com/intl/cms/s/0/4239e29e-02f2-11da-84e5-00000e2511c8-.html#axzz2fHrxwk9J> [Accessed 1/5/13]

Odittah and Isine 10 October 2011 *Leadership*

Odittah C and Isine I "Why FG Okayed Phone Bugging - Investigation" *Leadership* (10 October 2011)

Okonedo and Uzor 3rd January 2012 *Businessday*

Okonedo B and Uzor B "Nigeria Yearns for Broadband Internet in 2012" *Businessday* newspaper (3rd January 2012)

Available at <http://businessdayonline.com/NG/index.php/tech/78-computing/31485-nigeria-yearns-for-broadband-internet-in-2012> [Accessed 13/3/13]

Onuba February 14 February 2012 *Punch*

Onuba I "112.5 million Nigerians live in poverty – NBS" *Punch* newspaper (14 February 2012)

Available at <http://www.punchng.com/business/business-economy/112-5-million-nigerians-live-in-poverty-nbs/> [Accessed 12/6/12]

Oruame 23 June 2011 *The Nation*

Oruame S "Data protection in SIM Card Registration 2" *The Nation* newspaper (23 June 2011)

Available at <http://www.thenationonlineng.net/2011/index.php/business/10217-data-protection-in-sim-card-registration-2.html> [Accessed 3/1/12]

Osuagwu 6 September 2009 *The Vanguard*

Osuagwu P "Glo 1 Submarine Cable Lands in Lagos" *The Vanguard* newspaper (6 September 2009)

Available at <http://www.vanguardngr.com/2009/09/glo-1-submarine-cable-lands-in-lagos/> [Accessed 13/3/13]

P

***Punch* Editorial 18 November 2003**

Editorial "The Missing Okigbo Panel Report" *Punch* (18 November 2003)

R

***Red Herring* online magazine**

Available at <http:www.web.archive.org/web/2002022016085/http//www.redherring.com.-mag/issue76/mag-from-76.html> [Accessed 26/3/12]

S

Singer 16 June 2012 *The New York Times*

Singer N "You for Sale Mapping, and Sharing, the Consumer Genome" *The New York Time* newspaper (16 June 2012)

Available at <http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=1&ref=natashasinger> [Accessed 7/8/12]

Smith 7 February 2006 *The Guardian*

Smith H "Vodafone embroiled in Greek phone-tapping scandal" *The Guardian* online publication (7 February 2006)

Available at <http://www.guardian.co.uk/business/2006/feb/07/newmedia.media> [Accessed 23/12/11]

Sunday 31st May 2009 *Sunday Trust*

Sunday H O "Niger Delta: The albatross confronting Yar'adua's administration" *Sunday Trust* (31st May 2009)

Available at <http://sundaytrust.com.ng/index.php/news/11770-niger-delta-the-albatross-confronting-yaraduas-administration> [Accessed 23/12/12]

Shehu 5 July 2010 *ThisdayLive*

Shehu M "N55m Bribery Scandal: ICPC Drags Wabara, Osuji to Supreme Court" in *ThisdayLive* (5 July 2010)

Available at <http://www.thisdaylive.com/articles/n55m-bribery-scandal-icpc-drags-wabara-osuji-to-supreme-court/84082/> [Accessed 2/6/12]

T

Tagbo 17 February 2011 *Businessday*

Tagbo E "Telecoms overtakes banking, real sector in contribution to growth" *Businessday* (17 February 2011)

Available at <http://businessdayonline.com/NG/index.php/news/76-hot-topic/18278-telecoms-overtakes-banking-real-sector-in-contribution-to-growth>. [Accessed 27/12/11]

***The Week* Editorial Staff 20 June 2012**

Editorial Staff "Acxiom Corp: The 'faceless organization that knows everything about you'" *The Week* (20 June 2012)

Available at <http://theweek.com/article/index/229508/acxiom-corp-the-faceless-organization-that-knows-everything-about-you> [Accessed 17/9/12]

U

Uzor 3 January 2012 *Businessday*

Uzor B "Investment in network expansion solution to QoS challenge, says NCC" *Businessday* newspaper online (3 January 2012)

Available at <http://www.businessdayonline.com/NG/index.php/tech/78-computing/31484-investment-in-network-expansion-solution-to-qos-challenge-says-ncc> [Accessed 3/1/12]

V

***Vanguard* 14 January 2010**

Vanguard newspaper "Glo Sues NCC, MTN over Interconnection Dispute" (14 January 2010)

Available at <http://www.vanguardngr.com/2010/01/glo-sues-ncc-mtn-over-interconnect-dispute/> [Accessed 13/3/2013]

W

Williams 22 February 2013 *Dailytrust*

Williams S "Nigeria's new Trade Policy ready June" *Dailytrust* (22 February 2013)

Available at <http://www.dailytrust.com.ng/index.php/business/51168-nigeria-s-new-trade-policy-ready-june> [Accessed 6/5/13]

***Wired* 26 September 1999**

Wired (online magazine) "You have zero privacy anyway" (26 September 1999)

Available at: <http://www.wired.com/news/politics/0,1283,17538,00.html> [Accessed 4/3/13]

TABLE OF CASES

NIGERIA

Abdulhamid v Akar (2006) All FWLR (Pt 321) 1191

Achebe v Nwosu (2003) 7 NWLR (Pt 818) 103

Adesanya v President of Nigeria (1981) 1 All N L R 1

Adikwu & Ors v House of Representatives & Ors (1983) 4 N C L R 269

Akulega v Benue State Civil Service Commission & Anor (2002) 2 CHR 1

Bronik Motors Ltd v Wema Bank (1985) 6 NCLR 1

Cheranci v Cheranci (1960) NRNLR 24

Medical and Dental Practitioners Disciplinary Council v Dr. John E. N. Okonkwo (2001) 3 SC 92

DPP v Obi (1961) 1 All NLR 186

Eshugbayi Eleko v Officer Administering the Government of Nigeria (1931) AC 662

Fawehinmi v Abacha (1996) 9 NWLR (Pt 475) 75

J S Olawoyin v Att-Gen Northern Region (1961) 1 All NLR 269

Lekwot v Judicial Tribunal (1993) 2 NWLR (Pt 276) 410

Madu v Neboh & Anor (2002) 2 CHR 67

Nemi v State (1994) 9 NWLR (Pt 366) 1

Nwankwo v The State (1985) 6 NCLR 228

Ogugu v The State (1994) 9 NWLR (Pt 366) 1

Okeke v A-G Anambra State (1992)1 NWLR (Pt 215) 60

Onwo v Oko & Ors (1996) 6 NWLR (Pt 456) 584

R v Amalgamated Press Ltd (1961) 1 All NLR 199

Ransome-Kuti v Att-Gen of the Federation & Ors (1985) 16 NSCC (Pt 1) 879

Tukur v Govt of Gongola State (1989) 4 NWLR (Pt 117) 517

Ukaegbu v A-G Imo State (1984) 5 NCLR 78

AUSTRALIA

National Archives and Records Administration v Favish et al 124 S Ct 1570 (2004)

Chappell v TCN Channel Nine (1988) 14 NSWLR 153

AUSTRIA

Lingens v Austria (1986) 8 EHRR 407

CANADA

Jane Doe v Board of Commissioners of Police for the Municipality of Metropolitan Toronto et al Court File No 87-CQ-21670, Judgment July 3, 1998

Available at <http://www.c4pa.ca/wp-content/uploads/2010/12/Jane-Doe-v-TPSB-1998-SCJ.pdf>. [Accessed 15/4/13]

CHILE

Claude-Reyes et al v Chile (2006). Available at <http://www.corteidh.or.cr>. [Accessed 12/7/12]

FRANCE

Huvig v France 12 EHRR 528 1990

GERMANY

65 BVerfGE (Decisions of the Federal Constitutional Court) 1 42 (1983)

ICELAND

Thorgeir Thorgeirson v Iceland (1992) 14 EHRR 843

INDIA

S P Gupta v President of India and Others (1982) AIR (SC) 149

ITALY

Italy v Commission (1985) ECR 873

MOLDOVA

Sirbu and others v Moldova (Applications nos. 73562/01, 73565/01, 73712/01, 73744/01, 73972/01 and 73973/01) 15/06/2004

SOLOMON ISLANDS

Folatalu v A-G Solomon Islands (2003) CHR 279

SOUTH AFRICA

Bernstein v Bester NO 1996 (2) SA 751 (SCA)

Janit v Motor Industrial Fund Administrators (Pty) Ltd 1995 (4) SA 293 (A)

Klein v Attorney-General WLD 1995 (3) SA 848 (W)

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC)

S v A 1971 (2) SA 293 (T)

SWEDEN

Gillberg v Sweden (2010) ECHR 1676

Leander v Sweden (1987) 9 EHRR 433

TURKEY

Sener v Turkey (2003) 37 EHRR 34

UNITED KINGDOM

A v B Plc (2003) QB 195

AG v Guardian Newspapers (No 2) 1990) 1 AC 109

AG v Guardian Newspapers (1987) 1WLR 1248

Berezovsky v Forbes Inc (No 2) (2001) EMLR 1030

Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft mbH (1982) 1 All ER 293

Campbell v MGN Limited (2004) UKHL 22

Coco v AN Clark (Engineers) Ltd (1969) RPC 41

Derbyshire County Council v Times Newspapers Ltd (1993) AC 534

Douglas v Hello! Ltd (2001) 2 WLR 992 (CA)

Duke of Argyll v Duchess of Argyll (1967) 1 Ch 302

Ellis v Chief Constable Essex Police (2003) EWHC 1321

Entores Ltd v Miles Far East Corporation (1955) 2 All ER 493

Gordon Kaye v Andrew Robertson and Sport Newspapers Ltd (1991) FSR 62

Halford v United Kingdom 24 EHRR 523, 25 June 1997

Home Office v Wainright (2001) EWCA Civ 2081

Naomi Campbell v MGN Limited (2004) 2 AC 457 (HL)

Roche v United Kingdom (2006) 42 EHRR 30

R v Central Independent Television Plc (1994) Fam 192

Silver v United Kingdom 3 EHRR 475 1980

Stephens v Avery [1988] Ch 449

Steven Jaques & Co v Mclean (1880) 5 QBD 346

Sunday Times Ltd v UK (1979) 2 EHRR 245

Venables v News Group Newspapers (2001) Fam 430

W v Edgell (1990) Ch 59

Wainright v Home Office (2003) UKHL 53

UNITED STATES

Abrams v United States 250 US 616 (1919)

Barron v. Baltimore 32 U.S. 243 (1833)

Doe v Bolton 410 US 179 (1973)

Doe v Chao 540 US (2004) 614

Durkee v Vermont C Ry 29 Vt 127 (1856)

Eisenstadt v Baird 405 US 438 (1972)

Grosjean v American Press Co 297 US 233 240 (1936)

Gitlow v New York 268 US 652 (1925)

Griswold v Connecticut 381 US 479 (1965)

Houchins v KQED Inc 438 US 1 (1978)

Katz v United States 389 US 347 (1967)

Kyllo v United States 33 U.S. 27 (2001)

MCI v AT&T 708 F 2d 1081 (7th Circ) (1983)

New York Times v United States 403 U.S. 713 (1971)

New York Times Co v Sullivan 376 U.S. 254 (1964)

Oklahoma Press Pub Co v Walling 327 US 186 (1946)

Olmstead v United States 277 US 438 (1928)

Pell v Procunier 417 US 817 (1974)

Richmond Newspapers Inc v Virginia 448 US 555 (1980)

Roe v Wade 410 US 113 (1973)

Saxbe v Washington Post Co. 417 US 843 (1974)

Stanley v Georgia 394 US 557 (1969)

Sussman v US Marshals Serv 494 F 3d (DC Cir 2007) 1106

Trevor v Wood 36 NY 307, 93 Am Dec 262 (1867)

US v AT&T 524 F Supp 1336 (DC C) 1981

United States v Verdugo-Urquidez 494 US 259, 281 (1990)

United States v Yousef 327 F.3d 56 (2d Cir 2003)

United States v Yunis 924 F 2d 1086 (DC Cir 1991)

Whalen v Roe 429 US 589, 605 (1976)

TABLE OF STATUTES

NIGERIA

Advance Fee Fraud and other Fraud Related Offences Act, Laws of the Federation of Nigeria, 2006

African Charter (Ratification and Enforcement) Act, Laws of the Federation of Nigeria, 1990

Border Communities Development Agency (Establishment, Etc) Act, Laws of the Federation of Nigeria, 2003

Communications Act, Laws of the Federation of Nigeria, 2003

Constitution (Suspension and Modification) Decree No 107 of 1993

Corrupt Practices and Other Related Offences Act, Laws of the Federation of Nigeria, 2000

Criminal Code Act, Laws of the Federation of Nigeria, 1990

Criminal Procedure Act, Laws of the Federation of Nigeria, 1990

Criminal Procedure (Amendment) Act, Laws of the Federation of Nigeria, 2004

Customs and Excise Management Act, Laws of the Federation of Nigeria, 2003

Defamation and Offensive Publications Act, Laws of the Federation of Nigeria, 1990

Evidence Act, Laws of the Federation of Nigeria, 1990

Federal Inland Revenue Service (FIRS) Act, Laws of the Federation of Nigeria, 2007

Federal Military Government (Supremacy and Enforcement of Powers) Decree No 12 of 1994

Federal Road Safety Commission Act, Laws of the Federation of Nigeria, 2004

Fire Service Act, Laws of the Federation of Nigeria, 1990

Freedom of Information Act, Laws of the Federation of Nigeria, 2011

Independent National Electoral Commission (INEC) Act, Laws of the Federation of Nigeria, 1998

Interpretation Act, Laws of the Federation of Nigeria, 1990

Marriage Act, Laws of the Federation of Nigeria, 1990

Money Laundering (Prohibition) Act, Laws of the Federation of Nigeria, 2011

National Agency for Food and Drug Administration and Control (NAFDAC), Laws of the Federation of Nigeria, 1993

National Health Insurance Scheme (NHIS) Act, Laws of the Federation of Nigeria, 1999

National Identity Management Commission (NIMC) Act, Laws of the Federation of Nigeria, 2007

NESREA Act, Laws of the Federation of Nigeria, 2007

Nigerian Communications Commission Act, Laws of the Federation of Nigeria, 2000

Nigerian Communications Commission Act, Laws of the Federation of Nigeria, 2003

Nigerian Communications Commission (Amendment) Act, Laws of the Federation of Nigeria, 2000

Nigeria Postal Service Act, Laws of the Federation of Nigeria, 2004

Official Secrets Act, Laws of the Federation of Nigeria, 1990

Posts and Telecommunications Proceedings Act, Laws of the Federation of Nigeria, 1990

Public Complaints Commission Act, Laws of the Federation of Nigeria, 1990

Sale of Gods Act, Laws of the Federation of Nigeria, 1990

State Security (Detention of Persons) Act, Laws of the Federation of Nigeria, 1990

Statistics Act, Laws of the Federation of Nigeria, 2004

Telecommunications and Postal Offences Decree No 21, 1995, Laws of the Federation of Nigeria, 2000

Telecommunications and Postal Offences (Amendment) Decree, Laws of the Federation of Nigeria, 2000

Wireless Telegraphy Act, Laws of the Federation of Nigeria, 1990

Wireless Telegraphy Amendment Decree No 31, 1998, Laws of the Federation of Nigeria, 2000

Subsidiary legislation

Fundamental Rights (Enforcement Procedure) Rules, 2009

Constitution

Constitution of the Federation of Nigeria, 1960

Constitution of the Federal Republic of Nigeria, 1963

Constitution of the Federal Republic of Nigeria, 1979

Constitution of the Federal Republic of Nigeria, 1989

Constitution of the Federal Republic of Nigeria, 1993

Constitution of the Federal Republic of Nigeria, 1999

State Laws

High Court Law (Eastern Nigeria Laws 1963, Cap 61)

High Court Law (Northern Nigeria Laws 1963, Cap 49)

Law (Miscellaneous Provisions) Law (Laws of Lagos State, Cap 65 1973)

Law of England (Application) Law (Western Region of Nigeria Laws 1959, Cap 60)

Northern Region Children and Young Persons Law NR No 28 of 1958

AUSTRALIA

Privacy Act, 1988

Privacy Amendment (Private Sector) Act, No 155 (2000)

State law

Privacy and Personal Information Protection Act, 1998 of New South Wales

GHANA

Preventive Detention Act of 1958 (Ghana)

NEW ZEALAND

Privacy Act, 1993

Privacy (Cross-Border Information) Amendment Act, 2010

SINGAPORE

Infocomm Development Authority of Singapore Act No 41 of 1999

SOUTH AFRICA

Constitution of the Republic of South Africa Act 108 of 1996

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

UNITED KINGDOM

Data Protection Act, 1998

Freedom of Information Act, 2000

Financial Services and Markets Act, 2000

Human Rights Act, 1998

Subsidiary legislation

Environmental Information Regulations, 2004

Financial Conduct Authority (FCA) Handbook, 2013

UNITED STATES OF AMERICA

Cable Television Consumer Protection and Competition Act of 1992, Public Law 102-385, 106 Stat 1460

Children's Online Privacy Protection Act 15 USC §§ 6501–6506

Communications Act of 1934, Public Law 416, 47 USC § 151

Computer Matching and Privacy Act of 1988, Public Law 100-503, 102 Stat 2507 5 USC §552a

Computer Security Act of 1987, Public Law 100-235, 101 Stat 1724

Digital Millennium Copyright Act of 1998, Public Law 105-304, 112 Stat 2860

Fair Credit Reporting Act of 1968(as amended December 18, 2010). 15 USC § 1681

Federal Information Security Management Act (or Gramm-Leach-Bliley Act) of 1999, (Pub L 106–102)

Health Insurance Portability and Accountability Act of 1996, (Pub L 104-191)

Privacy Act of 1974, (Pub L 93–579, 88 Stat 1896), 5 USC § 552a

Telecommunications Act of 1996, (Public Law No 104-104), 110 Stat 56 (1996)

Trade Act of 1974 (Pub L 93–618) 19 USC § 2411