

THE REGULATION OF COMMUNICATIONS SURVEILLANCE IN NIGERIA

by

Tope Adefemi Osuntogun

Submitted in fulfilment of the requirements for the degree

Doctor Legum (LLD)

In the Faculty of Law,
Nelson Mandela University

August 2022

Promoter: **Professor Joanna Botha**


Co-Promoters: **Professor André Mukheibir**

Professor Adewale Taiwo

DECLARATION OF ORIGINALITY

I, the undersigned, hereby declare that this thesis, which I submit for the degree of Doctor Legum (LLD) in the Faculty of Law, Nelson Mandela University, is my own work and has not previously been submitted for a degree at another university.

I have correctly cited and acknowledged all my sources.

Student: 
Tope Adefemi Osuntogun

Date: 16 August 2022

DEDICATION

To Jesus Christ my solid rock and foundation. To my parents Mr. Adeyinka and Mrs. Abiola Osuntogun who encouraged me to pursue this degree and dedicated their all to ensure that I completed it. I am eternally grateful for your love and many sacrifices.

ACKNOWLEDGEMENTS

While writing this thesis, I received immense support for which I am very thankful. To my supervisors, Professors Joanna Botha, André Mukheibir and Adewale Taiwo, I am extremely grateful for your patience, ideas, feedbacks, constructive criticisms and for genuinely caring for my overall wellbeing during this process. I could not have completed this project without your support. I am also grateful to Professor Patrick Vrancken who together with Professor Joanna Botha facilitated the research hub which was of tremendous assistance in improving my research skills. I am grateful to Nelson Mandela University for providing me with the Research and Development bursary.

I am grateful to the former Vice Chancellor of Ajayi Crowther University, Rt. Rev. (Prof.) Dapo Asaju whose idea it was for me to study in South Africa and facilitated my study leave with pay. I acknowledge the support of the current Vice Chancellor and management of Ajayi Crowther University and the Dean and Heads of Departments of the Faculty of Law, Ajayi Crowther University, Professors Oladipo Solanke, Olanrewaju Onadeko (SAN) and Gaus Okwezuzu, who consistently supported me.

I appreciate my colleagues who provided valuable advice, Dr. Idowu Akinloye who read some of my drafts and provided valuable feedbacks. Also, to my study buddies Ntemesha Maseka, Rachel Chasakara and Priscilla Moyo who constantly exchanged ideas with me during the long, wintry study nights at the Ocean Sciences Campus.

To my uncles and aunties, Professor Adeniyi and Professor (Mrs) Bolanle Osuntogun, Professor and Dr. (Mrs) Abiodun Adediran, whose indelible achievements in academia and persistent nudges to follow their footsteps encouraged me to pursue this degree. And to my aunty, Mrs. Wuraola Adekanmbi, I appreciate your support.

To my siblings, Mr. Olutoyin and Barr. (Mrs.) Ademayowa Ogunmola, Adefisayo Osuntogun, Praise Osuntogun, Aderemi Adediran and Mrs. Olufunke Adebimpe, who consistently supported me, I am sincerely grateful for your love. Also, to Barr. Ibitayo Durosomo, Barr. Juliet Abah, Dr. Olufunmilayo Fagbadebo and Ms. Siphokazi Mazonda, your immeasurable love is appreciated.

Lastly, to my parents Mr. Adeyinka and Mrs. Abiola Osuntogun, I did not have to start from the bottom because you carried me on your shoulders. I am very grateful.

ACRONYMS AND ABBREVIATIONS

AAICJ	American Association for International Commission of Jurists
ACHPR	African Charter on Human and Peoples' Rights
ACtHR	African Court of Human and People's Rights
ACRWC	African Charter on the Rights and Welfare of the Child
AHRLJ	African Human Rights Law Journal
ANLR	All Nigerian Law Report
ANPP	All Nigeria Peoples Party
AU	African Union
AUCCP	African Union Convention on Cyber Security and Personal Data Protection
BCLR	Butterworths constitutional law report
CA	Court of Appeal
CBN	Central Bank of Nigeria
CC	Constitutional Court
CCPR	Consumer Code of Practice Regulation
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CPPA	Cybercrime (Prohibition, Prevention, etc) Act
CPA	Criminal Procedure Act
CPC	Criminal Procedure Code
CRA	Credit Reporting Act
CRC	Convention on the Rights of the Child
CSP	Communications service provider
DIA	Defence Intelligence Agency
DSS	Department of State Security Service

ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECOWAS	Economic Community of West African States
ECTA	Electronic Communications and Transaction Act
EFCC	Economic and Financial Crimes Commission
EHRR	European Human Rights Reports
EMTS	Emerging Markets Telecommunications Services Limited
EU	European Union
FHCLR	Federal High Court Law Report
FIP	Fair Information Practices
FOIA	Freedom of Information Act
FREP	Fundamental Rights (Enforcement) Procedure
GP	Gauteng Province
HRC	Human Rights Committee
IDEA	Institute for Democracy and Electoral Assistance
ICCPR	International Convention on Civil and Political Rights
ICT	Information and Communications Technology
ICRMW	International Convention on the Protection of the Rights of All Migrant Workers
IGP	Inspector General of Police
IJHSS	International Journal of Humanities and Social Sciences
IPA	Investigatory Powers Act
IPT	Investigatory Powers Tribunal
JAL	Journal of African Law
JSAL	Journal of South African Law
JSC	Judicial Service Commission

JSCI	Joint Standing Committee on Intelligence
LEA	Law enforcement agency
LEO	Law enforcement officer
LFN	Laws of Federation of Nigeria
LICR	Lawful Interception of Communications Regulation
LPELR	Law pavilion electronic law report
MGN	Mirror Group Newspaper Ltd
MOOC	Massive Open Online Course
NAUJILJ	Nnamdi Azikiwe University Journal of International Law and Jurisprudence
NCA	Nigerian Communications Act
NCC	Nigerian Communications Commission
NDLEA	National Drug Law Enforcement Agency
NDPR	Nigerian Data Protection Regulation
NHA	National Health Act
NIA	National Intelligence Agency
NIMC	National Identity Management Commission
NITDA	National Information Technology Development Agency
NSA	National Security Adviser
NSIA	National Strategic Intelligence Act
NWLR	Nigerian Weekly Law Report
OHCHR	Office of the High Commissioner on Human Rights
OIC	Office for Interception Centre
OJ	Official Journal
OSI	Office of the Surveillance Intermediary
PELR	Potchefstroom Electronic Law Report

POA	Public Order Act
POPIA	Protection of Personal Information Act
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
RTS	Registration of Telephone Subscribers
RTSR	Registration of Telephone Subscribers Regulation
SACR	South African Criminal Law Report
SALJ	South African Law Journal
SALR	South African Law Report
SADC	Southern African Development Community
SC	Supreme Court (Nigeria)
SCA	Supreme Court of Appeal (South Africa)
SR	Special Rapporteur
THRR	Transnational Human Rights Review
TPPA	Terrorism (Prevention and Prohibition) Act
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
US	United States of America
WHO	World Health Organization

TABLE OF CONTENTS

	Page
DECLARATION OF ORIGINALITY	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
ABSTRACT	xvi
CHAPTER ONE:INTRODUCTION	1
1.1 Introduction.....	1
1.2 Problem statement.....	5
1.3 Legal background.....	9
1.3.1 International law on the right to privacy and communications surveillance.....	9
1.3.2 Regional laws on the right to privacy and communications surveillance	11
1.3.2.1 African regional law on the right to privacy and communications surveillance.....	11
1.3.2.2 European regional law on the right to privacy and communications surveillance.....	12
1.3.3 Sub-regional laws on the right to privacy and communications surveillance ...	13
1.3.3.1 Economic Community of West African States.....	13
1.3.3.2 Southern African Development Community.....	14
1.3.4 The legal framework on the right to privacy and communications surveillance in South Africa.....	14
1.3.4.1 The constitutional protection of the right to privacy and limitation of rights...15	
1.3.4.2 The common law.....	16
1.3.4.3 Legislative framework of communications surveillance in South Africa.....	17
1.3.5 The legal framework on the right to privacy and communications surveillance in Nigeria.....	18
1.3.5.1 Constitutional protection of the right to privacy and its limitation.....	18
1.3.5.2 Legislative framework of communications surveillance in Nigeria.....	19
1.3.5.2.1 Nigerian Communications Act.....	19
1.3.5.2.2 Lawful Interception of Communications Regulation.....	21
1.3.5.2.3 Cybercrimes (Prohibition, Prevention, Etc) Act.....	22
1.3.5.2.4 Terrorism (Prevention and Prohibition) Act, 2022 (TPPA).....	23
1.3.5.3 Summary of the problems with the Nigerian legislative framework on communications surveillance.....	24
1.3.5.3.1 Lack of a comprehensive statute.....	25
1.3.5.3.2 Ineffective procedural and inadequate guidelines at all stages of communications surveillance.....	25
1.3.5.3.3 Ineffective oversight mechanisms for communications surveillance.....	26
1.3.5.3.4 An effective avenue for redress.....	26
1.4 Aims and objectives of the study.....	26
1.5 Research questions.....	27
1.6 Methodology.....	28
1.7 Limitations of the study.....	29
1.8 Significance of the Study.....	30
1.9 Chapter summary.....	30
CHAPTER TWO: INTERNATIONAL, REGIONAL AND SUB-REGIONAL LAW ON THE REGULATION OF COMMUNICATIONS SURVEILLANCE	32

2.1 Introduction.....	32
2.2 International law on the right to privacy.....	33
2.2.1 The Universal Declaration of Human Rights.....	34
2.2.2. International Covenant on Civil and Political Rights.....	37
2.2.2.1 The 1988 UN Human Rights Committee CCPR General Comment No. 16 on article 17 (General Comment 16).....	39
2.2.2.2 The Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR.....	41
2.2.2.3 Right to privacy in the ICCPR.....	43
2.2.2.4 Protection of correspondence and communication.....	43
2.2.2.5 Interference with privacy and/or correspondence.....	44
2.2.2.5.1 Unlawful interference with privacy and correspondence.....	45
2.2.2.5.2 Arbitrary interference with privacy and correspondence.....	48
(i) Proportionality.....	50
(ii) Necessary.....	51
2.2.3 The United Nations Convention on the Rights of the Child.....	51
2.2.4 The International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families.....	53
2.2.5 The need for a new General Comment on article 17.....	54
2.3 African regional laws on the regulation of communications surveillance.....	55
2.3.1 The African Charter on Human and People’s Rights.....	56
2.3.2 The African Charter on the Rights and Welfare of the child.....	58
2.3.3 The African Union Convention on Cyber Security and Personal Data.....	59
2.3.4 The Declaration on Freedom of Expression and Access to Information.....	62
2.3.4.1 The protection of the right to privacy in the 2019 Declaration.....	62
2.3.4.2 Limitation of right to privacy in the 2019 Declaration.....	64
2.3.5 The jurisdiction of the ACtHR in respect of right to privacy adjudication.....	65
2.4 African sub-regional laws on the right to privacy.....	66
2.4.1 The Supplementary Act on Personal Data Protection within the Economic Community of West African States 2010.....	66
2.4.2 Southern African Development Community model law on data protection.....	67
2.4.3 Justification for the study of European regional law.....	70
2.5 European regional laws on communications surveillance.....	70
2.5.1 European Convention on Human Rights.....	71
2.5.1.1 Communications surveillance being “in accordance with the law”.....	73
2.5.1.2 Communications surveillance must be necessary in a democratic society...74	
2.5.1.2.1 Competent oversight body.....	75
2.5.1.2.2 Duration of surveillance.....	77
2.5.1.2.3 An effective avenue for redress.....	78
2.5.1.3 Legitimate aims for communications surveillance.....	80
2.5.2 The Charter of Fundamental Rights of the European Union.....	82
2.6 Conclusion.....	86
CHAPTER THREE: AN ANALYSIS OF THE LEGAL FRAMEWORK OF COMMUNICATIONS SURVEILLANCE IN SOUTH AFRICA.....	89
3.1 Introduction.....	89
3.2 Importance of South African jurisprudence to the study and the links between South Africa and Nigeria.....	91
3.3 Constitutional framework in South Africa.....	92
3.3.1 Constitutional values.....	92
3.3.2 Legality of laws in the South African context.....	93

3.3.3 Openness and accountability	94
3.4 Constitutional protection of the right to privacy in South Africa.....	96
3.5 The right to privacy of communications.....	100
3.6 Limitation of rights in the Constitution.....	101
3.6.1 Overview of section 36 of the Constitution.....	101
3.6.2 Reasonability and justifiability of limitations of rights.....	102
3.6.2.1 The nature of the right.....	104
3.6.2.2 The importance of the purpose of the limitation.....	104
3.6.2.3 The nature and extent of the limitation.....	105
3.6.2.4 The relation between the limitation and its purpose.....	106
3.6.2.5 Less restrictive means to achieve the purpose.....	106
3.7 Invasion of privacy in terms of the South African common law.....	107
3.7.1 Overview of the common law protection of privacy.....	107
3.7.2 Wrongfulness and communications surveillance.....	108
3.7.3 The Bill of Rights and the common law.....	110
3.7.4 The common law and constitutional relief.....	112
3.8 Statutory regulation of communications surveillance in South Africa.....	114
3.8.1 Overview of legislative regulation of communications surveillance in South Africa.....	114
3.8.2 The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002.....	115
3.8.2.1 Brief outline of the sections.....	115
3.8.2.2 Objective of the RICA.....	115
3.8.2.3 Selected terms in the RICA defined.....	117
3.8.2.4 The structural and substantive framework of the RICA.....	118
3.8.2.5 The problematic provisions in the RICA.....	122
3.8.2.5.1 The problems in the RICA as canvassed in <i>AmaBhungane v Minister of Justice</i>	123
(i) Overview of the applicants' arguments.....	123
(ii) High Court and Constitutional Court Orders.....	124
(iii) Infringement on the right of access to court.....	125
(iv) Infringement on the right to a fair hearing.....	128
(a) The independence and appointment of designated judges	128
(b) The procedure for an application for surveillance directions	130
(v) Unlawful processing of post-surveillance information	135
(vi) Infringement on the right to freedom of expression and fair trial.....	140
(vii) Unlawful utilisation of untargeted (bulk) surveillance	140
3.8.2.5.2 Brief overview of additional problematic areas in the RICA.....	141
(i) Lesser protection for communication-related information in other statutes.....	142
(ii) Lesser protection for archived communication-related information.....	143
(iii) Difference in the requirements for application of intercept and communication-related direction.....	144
(iv) Interception of communication where a law enforcement officer participates in the communication.....	144
3.8.2.5.3 New issues in the RICA arising from the Constitutional Court's decision in <i>AmaBhungane v Minister of Justice</i>	145
(i) Absence of differentiation between intimate and non-intimate personal communications.....	146
(ii) Lack of distinction between communications related or non-related to interception.....	146

(iii) Lack of protection of the fundamental rights of collateral victims.....	147
(iv) Special protection for certain categories of persons during communications surveillance.....	148
3.8.2.6 Report of the Designated Judge on the authorisation of interception directions.....	150
3.8.3 The Protection of Personal Information Act, 2013.....	151
3.8.4 The Electronic Communications and Transactions Act, 2002.....	156
3.8.5 The Criminal Procedure Act, 1977.....	158
3.8.6 The Cybercrimes Act, 2020.....	162
3.9 Summary of the main features of legislative framework of communications surveillance in South Africa.....	164
3.10 Conclusion.....	165
CHAPTER FOUR.....	168
THE LEGAL FRAMEWORK OF COMMUNICATIONS SURVEILLANCE IN NIGERIA.....	168
4.1 Introduction.....	168
4.2 Brief history of the Nigerian Constitution.....	168
4.3 Supremacy of the 1999 Nigerian Constitution.....	171
4.4 The Bill of Rights in the 1999 Nigerian Constitution.....	173
4.4.1 Horizontal application of the Bill of Rights.....	175
4.4.2 Enforcement of the Bill of Rights.....	177
4.5 Constitutional protection of the right to privacy.....	178
4.6 Limitation of constitutional rights.....	179
4.6.1 Any Law.....	181
4.6.2 Reasonably justifiable in a democratic society.....	183
4.6.3 Legitimate aims for limiting constitutional rights in the 1999 Nigerian Constitution.....	188
4.6.3.1 Defence.....	190
4.6.3.2 Public morals.....	192
4.6.3.3 Public health.....	193
4.6.3.4 Public order and public safety.....	194
4.6.3.5 For the purpose of protecting the rights and freedom of other persons.....	196
4.6.4 The lack of objective interpretation of the legitimate aims.....	196
4.7 The common law and the right to privacy in Nigeria.....	197
4.8 Laws regulating communications surveillance in Nigeria.....	201
4.8.1 Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.....	203
4.8.2 Terrorism (Prevention and Prohibition) Act, 2022.....	207
4.8.3 Nigerian Communications Act, 2003.....	210
4.8.4 Lawful Interception of Communications Regulation, 2019.....	214
4.8.4.1 Structure of the Lawful Interception of Communications Regulation.....	215
4.8.4.2 Potentially sound provisions in the LICR.....	215
4.8.4.3 Problems with the LICR.....	217
4.8.4.3.1 Overreach into the exclusive legislative list.....	217
4.8.4.3.2 Broad powers of law enforcement agents.....	218
4.8.4.3.3 Inadequate protection of personal information.....	219
4.8.4.3.4 Optional warrant for interception of communication.....	220
4.8.4.3.5 Lack of clarity on the definition of unlawful interception of communication.....	221
4.8.4.3.6 Purposes for interception of communications infringe on the 1999 Nigerian Constitution.....	222

4.8.4.3.7 Inadequate experience of Judges on the special nature of intercept warrants.....	223
4.8.4.3.8 Application for warrant infringes unjustifiably on the right to fair hearing..	225
4.8.4.3.9 Unjustifiable infringement on the right of access to court.....	226
4.8.5 Nigerian Data Protection Regulation, 2019.....	227
4.9 Conclusion.....	229
CHAPTER FIVE.....	233
RECOMMENDATION FOR A HUMAN RIGHTS BASED LEGAL FRAMEWORK ON COMMUNICATIONS SURVEILLANCE FOR NIGERIA.....	233
5.1 Introduction.....	233
5.2 The limitation clause must be correctly interpreted and provide a uniform guidance for limiting rights.....	235
5.2.1. An analysis of “reasonably justifiable” for human rights adjudication in Nigeria.....	236
5.2.1.1 International law standard on defining “reasonable”.....	237
5.2.1.2 African regional law on defining “proportionate” and “necessary”.....	240
5.2.1.3 South African approach to the limitation of rights.....	241
5.2.1.4 Recommendation for Nigeria on interpreting the limitation of rights.....	243
5.2.2 Legitimate aims must be clearly defined in the 1999 Nigerian Constitution...	243
5.2.2.1 International law standard for listing ‘legitimate aims’.....	244
5.2.2.2 South African approach for listing ‘legitimate aims’.....	246
5.2.2.3 Recommendations for listing ‘legitimate aims’.....	247
5.3 A comprehensive statute on communications surveillance in Nigeria.....	248
5.3.1. Lack of clarity of laws regulating communications surveillance.....	248
5.3.1.1 Conflicting provisions in the laws.....	248
5.3.1.2 The problem of foreseeability.....	250
5.3.1.3 International law standard for regulating clear domestic laws on communications surveillance.....	252
5.3.1.4. Regional law standard for regulating clear domestic laws on communications surveillance.....	253
5.3.1.4.1. African regional law standard for regulating clear domestic laws on communications surveillance.....	254
5.3.1.4.2 European regional law standard for regulating clear domestic laws on communications surveillance.....	255
5.3.1.5 South African approach to regulating clear laws on communications surveillance.....	257
5.3.1.6 Recommendations for regulating a clear law on communications surveillance in Nigeria.....	260
5.3.2 Lack of accessibility of the laws – public participation in law-making	262
5.3.2.1 International law standard for accessibility of laws regulating communications surveillance.....	263
5.3.2.2 European regional law standard for accessibility of laws regulating communications surveillance.....	264
5.3.2.3 South African approach on accessibility of laws regulating communications surveillance.....	264
5.3.2.4 Recommendations for Nigeria on accessibility of laws regulating communications surveillance.....	265
5.3.3 Overreach of the laws regulating communications surveillance in Nigeria	266
5.3.3.1 International law standard on overreach of the laws regulating communications surveillance.....	267

5.3.3.2 Regional and foreign law standard on overreach of laws regulating communications surveillance.....	268
5.3.4 Lack of safeguards for the acquisition of the metadata of communications...	268
5.3.4.1 International law standard on the acquisition of metadata.....	269
5.3.4.2 European regional jurisprudence on the acquisition of metadata.....	270
5.3.4.3 South African approach on the acquisition of metadata.....	271
5.3.4.4 Recommendation for Nigeria on the acquisition of metadata.....	272
5.4 The development and implementation of sound and fair procedural rules at all stages of communications surveillance.....	273
5.4.1 Problems with the pre-surveillance stage.....	274
5.4.1.1 The provision of the TPPA on the pre-surveillance stage.....	274
5.4.1.2 The provision of the CPPA on the pre-surveillance stage.....	275
5.4.1.3 The provisions of the LICR on the pre-surveillance stage.....	276
5.4.1.4 International law standard on the pre-surveillance stage.....	278
5.4.1.5 African regional law standard on the pre-surveillance stage.....	280
5.4.1.6 European regional law standard on the pre-surveillance stage.....	281
5.4.1.7 South African approach on the pre-surveillance stage.....	284
5.4.1.8 Recommendation for Nigeria on the regulation of the pre-surveillance stage of communications surveillance.....	287
5.4.2 The problems with the implementation stage of communications surveillance in Nigeria.....	288
5.4.2.1 European regional law standard on communications surveillance.....	290
5.4.2.2 South African approach on the implementation of communications surveillance.....	292
5.4.2.3 Recommendation for Nigeria on the implementation of communications surveillance.....	294
5.4.3 The post-surveillance stage of communications surveillance in Nigeria	294
5.4.3.1 European regional law standard on the post-surveillance stage of communications surveillance.....	296
5.4.3.2 South African approach on the post-surveillance stage of communications surveillance.....	298
5.4.3.3 Recommendation for the post-surveillance stage of communications surveillance.....	299
5.5 Independent and effective oversight mechanisms for communications surveillance.....	300
5.5.1 The problem with the oversight mechanisms for communications surveillance.....	300
5.5.2 International law on instituting oversight bodies.....	302
5.5.3 Regional law on instituting oversight bodies.....	303
5.5.3.1 African regional law on instituting oversight bodies.....	303
5.5.3.2 European regional law on instituting oversight bodies.....	303
5.5.4 South African approach on instituting oversight bodies.....	306
5.5.5 Recommendation for Nigeria on instituting oversight bodies.....	309
5.6 An effective avenue for redress.....	310
5.6.1 International law standards for an effective avenue for redress.....	310
5.6.2 Regional law for an effective avenue for redress.....	312
5.6.2.1 African regional law for an effective avenue for redress.....	312
5.6.2.2 European regional law for an effective avenue for redress.....	312
5.6.3 South African approach for an effective avenue for redress.....	314
5.6.4 Recommendation for Nigeria for an effective avenue for redress.....	315

5.7 Conclusion.....	316
CHAPTER SIX.....	319
6.1 Introduction.....	319
6.2 Research question one – The importance of right to communications’ privacy in the digital age.....	319
6.3 Research question two – International and regional law standards on the regulation of communications surveillance.....	320
6.4 Research question three – The lessons for Nigeria from the South African legal framework on communications surveillance.....	322
6.5 Research question four – The need for a comprehensive statute regulating communications surveillance in Nigeria.....	325
6.6 Research question five – The recommendations for the reform of the legal framework of communications surveillance in Nigeria.....	327
6.7 Main research question.....	330
6.8 Conclusion.....	331
BIBLIOGRAPHY.....	333
TABLE OF INTERNATIONAL INSTRUMENTS.....	333
TABLE OF LEGISLATION.....	335
TABLE OF CASES.....	338
DECISIONS OF INTERNATIONAL BODIES.....	338
BOOKS AND CHAPTERS IN BOOKS.....	350
JOURNAL ARTICLES.....	355
CONFERENCE PAPERS.....	369
THESES.....	370
REPORTS.....	370
ONLINE RESOURCES.....	372

ABSTRACT

This study examines the manner in which communications surveillance is regulated in Nigeria, with the aim of providing recommendations to ensure a new surveillance regime that provides adequate safeguards for human rights, particularly the right to privacy. The rapid innovation in ICT has brought new challenges to the right to privacy, among which is communications surveillance.

Communications surveillance is an important tool of law enforcement as it enables remote gathering of evidence through interception of communication and acquisition of the metadata of electronic communications. Communications surveillance could therefore be an egregious intrusion on a person's intimate private sphere and should only be permitted only when necessary. The clandestine nature of communications surveillance, however, increases the risk of unlawfulness as a person under surveillance will be unable to challenge the process unless they are notified.

The benchmark in international law is that laws regulating communications surveillance must be lawful, non-arbitrary and provide adequate safeguards for the right to privacy. This study establishes that the legal framework on communications surveillance in Nigeria does not meet this standard. Using the South African legal framework as a comparator and drawing on relevant international and regional law on the right to privacy and communications surveillance, this study recommends reforms for the current legal framework on communications surveillance in Nigeria.

KEYWORDS: communications surveillance, electronic communications, human rights, Nigerian Constitution, privacy, legal framework, recommendations, reforms, South African Constitution.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The objective of this thesis is to recommend reform for the legal framework of communications surveillance in Nigeria.

Communication is an important tool used to transfer information between people. Each century has seen new ways of improving communications by creating technologies that strive to eliminate barriers to the free flow of information.¹ Technology has been utilised in various forms to achieve different levels of improvement in the transfer of information. The 19th and 20th centuries witnessed the invention of various information and communications technologies (ICT), including the telephone, facsimile (fax) machine, intranet, camera, television, radio, computers and the internet.² The 21st century is known as the digital age because of advances in ICT that introduced the internet and digitisation.³ Digital communications technology currently plays a major role in the daily lives of people.⁴

¹ Caron and Caronia *Moving Cultures: Mobile Communication in Everyday Life* (2007) 3; Ross "Privacy in the Facebook Era: A South African Legal Perspective" 2012 129 *The South African Law Journal* 375.

² Manacorda and Tesei "Liberation Technology: Mobile Phones and Political Mobilization in Africa" 2020 88 *Econometrica, Economic Society Data* 564; Bilchitz "Privacy, Surveillance and the Duties of Corporation" 2016 1 *Journal of South African Law* 45; Tene "Privacy: The New Generations" 2011 1 *International Data Privacy Law* 16-19; Solove *The Digital Person: Technology and Privacy in the Information Age* (2004) 2, 22-26; DeVries "Protecting Privacy in the Digital Age" 2003 18 *Berkeley Technology Law Journal* 285; Berman and Mulligan "Privacy in the Digital Age" 1999 23 *Nova Law Review* 522. The International Telecommunication Union defines the internet of things as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based in existing and evolving interoperable information and communication technologies"; Saint and Garba *Technology and Policy for the Internet of Things in Africa* paper presented at Telecommunications Policy Research Conference 44: The 44th Research Conference on Communication, Information and Internet Policy (September 30 - October 1 2016) 1.

³ Albers "Surveillance and Data Protection Rights: Data Retention and Access to Telecommunications Data" in Albers and Sarlet (eds) *Personality and Data Protection Rights on the Internet* (2022) 69; Waldo and Millet (eds) *Engaging Privacy and Information Technology in Digital Age* (2007) 2; Katz "Mobile Communication and the Transformation of Daily Life: The Next Phase of Research on Mobiles" 2006 19 *Knowledge Technology and Policy* 64.

⁴ Bélanger and Crossler "Privacy in the Digital Age: A Review of the Information Privacy Research in Information Systems" *Management and Information Science (MIS) Quarterly* 2011 35 1018; Pillay *The Right to Privacy in the Digital Age: Opening Remarks at the United Nations High Commissioner for Human Rights to the Expert Seminar, Geneva, (February 2014)* 1.

In 1890, Warren and Brandeis argued for the protection of privacy as a right.⁵ Their arguments and those of other scholars, for the recognition of the right to privacy in the 19th and 20th centuries, resulted from the intrusion on privacy caused by the technological inventions of their time.⁶ These arguments in favour of the right to privacy yielded results, as privacy is now recognised globally as either an economic right or a human right.⁷

The privacy debates of the 21st century, which include debates concerning data privacy and communications surveillance, are tailored towards the right to privacy of persons utilising electronic communications, also known as the right to privacy in the digital age.⁸ There is a general consensus in these debates that the right to privacy should be protected as much on-line as it is off-line.⁹ This consensus is reflected in various statutes and international agreements that have mandated companies like

⁵ Warren and Brandeis "The Right to Privacy" 1890 4 *Harvard Law Review* 193-220.

⁶ Kalven "Privacy in the Tort Law—Were Warren and Brandeis Wrong?" 1966 31 *Law and Contemporary Problems* 327; Prosser "Privacy" 1960 48 *California Law Review* 385; Palmer "Privacy and the Law" 1975 *The New Zealand Law Journal* 747; Bloustein "Privacy as an aspect of Human Dignity: An Answer to Dean Prosser, 1961 39 *New York University Law Review* 962.

⁷ Zhang, Luo, Wang, Chen and Chen "'A Right to be Forgotten': Retrospective Privacy Concerns in Social Networking Services" 2022 *Behaviour & Information Technology* 2; Makulilo "One Size Fits All": Does Europe Impose its Data Protection Regime on Africa?" 2013 7 *Datenschutz und Datensicherheit* 448; the protection of the right to privacy from the United States' view is that privacy should stem from a concept of liberty thus its protection should be an economic right. The European Union views privacy from a concept of dignity and so protects privacy as a human right; Westin "The Origins of Modern Claims of Privacy in Philosophical Dimensions of Privacy" in Schoeman (ed) *An Anthropology* (1984) 56; Robert "Three Concepts of Privacy" 2001 89 *Georgetown Law Journal* 2089; Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" 2004 113 *The Yale Law Journal* 1153; Levin and Abril "Two Notions of Privacy Online" 2009 11 *Vanderbilt Journal of Entertainment and Technology Law* 1008.

⁸ Solove "Understanding Privacy" 2008 *The George Washington University Law School Public Law and Legal Theory Working Paper No.420* 8; Solove "I've Got Nothing to Hide" and other Misunderstandings of Privacy" 2007 44 *San Diego Law Review* 745; DeCew *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (1997) 1; McCreary "What Was Privacy?" 2008 86 *Harvard Business Review* 123; King "On-line Privacy in Europe – New Regulation for Cookies" 2003 11 *Journal of Information and Communication Technology Law* 225; Bamberger and Deirdre, "Privacy in Europe: Initial Data on Governance Choices and Corporate Practices" 2013 81 *George Washington Law Review* 1532; Makulilo "One Size Fits All: Does Europe Impose its Data Protection Regime on Africa?" 2013 7 *DuD.Datenschutz und Datensicherheit* 447; Abdulrauf and Daibu "New Technologies and the Right to Privacy in Nigeria: Evaluating the Tension between Traditional and Modern Conceptions" 2016 7 *Nnamdi Azikwe University Journal* 113; Neethling "The Concept of Privacy in South African Law" 2005 122 *SALJ* 20.

⁹ Nyst and Falchetta "The Right to Privacy in the Digital Age" 2017 9 *Journal of Human Rights Practice* 105; Pillay *The Right to Privacy in the Digital Age* (February 2014) Opening Remarks by the United Nations High Commissioner for Human Rights to the Expert Seminar Geneva 1; United Nations General Assembly Resolution the Right to Privacy in the digital age, 68th session, agenda 69(b), A/RES/68/167, 21 January 2014, 2; Milanovic "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" 2015 56 *Harvard International Law Journal* 85.

Facebook and Google to improve their privacy settings in order to reflect the right to privacy on-line.¹⁰

The widespread innovations in information and communications technology (ICT) have impacted positively on the mode of communication between people. For example, the telephone was replaced by internet-enabled mobile phones and fax-machines and telegrams were replaced by electronic mail (emails). These replacements have resulted in a faster and more effective means of communicating. The innovations were, however, accompanied by “[s]ubtler and more far-reaching means of invading privacy” one of which is communications surveillance.¹¹ Others include artificial intelligence, big data and video surveillance. Surveillance of various modes of communications is “almost as old as our ability to communicate”.¹² However, the traditional methods of surveillance, which include bugging, interception of letters and eavesdropping, are not as sophisticated and intrusive as the surveillance of electronic communications referred to as “communications surveillance”.¹³

Communications surveillance refers to any activity that results in the acquisition and interception of the content of communications and/or any acquisition of the metadata of an electronic communication.¹⁴ Metadata refers to information automatically generated during an electronic communication and includes the time of the

¹⁰ The Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.223); Council of Europe Data Protection Convention 108; European Union General Data Protection Regulation 2016/679; The African Union Convention on Cyber Security and Protection of Personal Data (2014); The United States Electronic Communications Privacy Act, 1986.

¹¹ *Olmstead v United States*, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting); Hosein and Palow “Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques” 2013 74 *Ohio State Law Journal* (OSLJ) 1072; Privacy international explanatory document on phone monitoring (May 2018) <https://privacyinternational.org/explainer/1640/phone-monitoring> (accessed 2019-02-01); Straw “*Interception of Communication in the United Kingdom: A Consultation Paper Presented by the Secretary of State for the Home Department by Command of Her Majesty* (June 1999) 1; Other intrusive innovation on privacy include artificial intelligence, big data and video surveillance.

¹² Hosein and Palow “Modern Safeguards for Modern Surveillance” 2013 OSLJ 1073.

¹³ Hosein and Palow “Modern Safeguards for Modern Surveillance” 2013 OSLJ 1074; Kerr “The Case for the Third-Party Doctrine” 2009 209 *Michigan Law Review* 572.

¹⁴ There is no generally accepted definition for communications surveillance. It is the law-makers responsibility to determine the meaning of the word “intercept/surveillance” in the legislation on the interception of communications. The United States’ Wiretap Act 18 *United States Congress § 2510(4) (2000)* defines intercept as “the aural acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device”; Section 183 of the Canadian Criminal Code Part VI defines intercept as including “listen to, record or acquire a communication or acquire the substance, meaning, or purport thereof”; Hosein and Palow “Modern Safeguards for Modern Surveillance” 2013 OSLJ 1076.

communication, the location of the parties to the communication and the duration of the communication.¹⁵ Interception of communications generally refers to the acquisition of the content of an electronic communications only. When the acquisition of metadata is included, the act is referred to as communications surveillance.¹⁶

Communications surveillance limits the right to privacy by interfering with private communications that are transmitted over electronic communications networks.¹⁷ Nevertheless, communications surveillance is an important tool in combatting crime and protecting national security, as it provides an avenue for gathering information that is useful for preventing, detecting and prosecuting terrorist activities. As a result of the highly intrusive nature of communications surveillance on the right to privacy, it is important to ensure that its use is regulated with a “clear legal framework” that safeguards against abuse and provides adequate protection for human rights.¹⁸

Communications surveillance is usually a clandestine operation and it is easy to manipulate for unlawful purposes as the surveillance subjects (persons under surveillance) are not aware that they are being monitored.¹⁹ As a result of the clandestine nature of surveillance, the surveillance subject is usually unable to challenge the procedure.²⁰ It is therefore important to ensure that the laws regulating surveillance are enacted to protect human rights proactively. One of the ways to

¹⁵ Michael Why *Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era* Law, Privacy and Surveillance in Canada in the Post-Snowden Era, Geist (ed), (2015) University of Ottawa Press 229; National Information Standards Organization, “Understanding Metadata,” (2004) *NISO Press*, <https://www.niso.org/publications/understanding-metadata-2017> (accessed 2021-01-10); Blumberg and Eckersley “On locational privacy, and how to avoid losing it forever” (August 2009) *White Paper, Electronic Frontier Foundation*, <https://www.eff.org/files/eff-locational-privacy.pdf> (accessed on 2021-04-23) 1; Hunter “Track and Trace, Trial and Error: Assessing South Africa’s Approaches to Privacy in Covid-19 Digital Contact Tracing” 2009 *The Media Policy and Democracy Project* 1.

¹⁶ Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 27th session, agenda items 2 and 3, A/HRC/27/37, 30 June 2014, (2014 OHCHR Report) paras [14, 19].

¹⁷ Straw “*Interception of Communication in the United Kingdom*” A Consultation Paper Presented by the Secretary of State for the Home Department by Command of Her Majesty (June 1999) 1.

¹⁸ Hosein and Palow “Modern Safeguards for Modern Surveillance” 2013 *OSLJ* 1073, 1083.

¹⁹ Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 39th session, agenda items 2 and 3, A/HRC/39/29, 3 August 2018, (2018 OHCHR report) par [40].

²⁰ (2018 OHCHR report) par [41].

regulate communications surveillance in a proactive manner is to ensure that domestic laws comply with international best practices on surveillance.²¹

1.2 Problem statement

Intensified state communications surveillance stems, in the main, from the terrorist attack on the United States of America (the US) that occurred on 9 September 2001 (“9/11”).²² Following 9/11, there was a perceived increased urgency to combat terrorism in the US and as a result the US Congress enacted laws to empower the State to implement communications surveillance.²³ However, as explained below, the infamous Snowden revelations subsequently made it clear that the US had overreached its powers and conducted unlawful surveillance on several occasions.²⁴

²¹ Hosein and Palow “Modern Safeguards for Modern Surveillance” 2013 OSLJ 1073 1075.

²² Bergen P. “September 11 Attacks” <https://www.britannica.com/event/September-11-attacks> (accessed 2022-11-21). “September 11 attacks, also called 9/11 attacks, series of airline hijackings and suicide attacks committed in 2001 by 19 militants associated with the Islamic extremist group al-Qaeda against targets in the United States, the deadliest terrorist attacks on American soil in U.S. history. The attacks against New York City and Washington, D.C., caused extensive death and destruction and triggered an enormous U.S. effort to combat terrorism. Some 2,750 people were killed in New York, 184 at the Pentagon, and 40 in Pennsylvania (where one of the hijacked planes crashed after the passengers attempted to retake the plane); all 19 terrorists died. Police and fire departments in New York were especially hard-hit: hundreds had rushed to the scene of the attacks, and more than 400 police officers and firefighters were killed.”

²³ Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511, 92 Stat. 26 (1978) (codified as amended in scattered sections of 50 U.S.C.); Protect America Act of 2007, Public Law No. 110-55, 121 Stat. 552 (2007); Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Public Law No. 110-261, 122 Stat. 2436, 2437-78 (2008) (to be codified in 50 U.S.C. ss. 1801-12); Balkin “The Constitution in the National Surveillance State” 2008 93 *Minnesota Law Review* 2.

²⁴ Edward Snowden was an employee of the National Security Agency (NSA) who revealed classified information concerning the collection of telecommunications metadata. He revealed this information to a British Newspaper, The Guardian. The information was published on 6 June 2013. It concerned a secret “program to collect domestic telecommunications metadata...from Verizon Business Networks Services. A day later, the paper revealed details about PRISM, an NSA program that targeted the Internet communications and stored data of ‘non-US persons’ outside the US and those communicating with them, and the extent to which US companies cooperate with the government. More leaks followed, with details about the US government spying on Chinese computers, news that the NSA and its British counterpart GCHQ had used a monitored Internet cafe to eavesdrop on the communications of political leaders attending the 2009 London G20 summit, that the British were themselves conducting massive intercepts of domestic communications, and that the NSA had been collecting metadata from domestic Internet communications.” Edward Snowden, on indicating his concern over the NSA’s collection of personal data stated that “[w]hen you see everything, you see them on a more frequent basis, and you recognize that some of these things are actually abuses ... eventually you realize these things need to be determined by the public, not by somebody who is merely hired by the government”. See too Landau “Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelation” (July/August 2013) *IEEE Security and Privacy* 66. Landau “Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelation” (July/August 2013) *IEEE Security and Privacy* 66; Orwell *1984* (1949). Snowden’s revelation showed state abuse of

The gaps in the regulation of communications surveillance became a global issue with the revelation by Snowden that the US, the United Kingdom (UK), Canada, Australia and New Zealand, referred to as the “Five Eyes”, had subjected several persons and organisations to surveillance.²⁵ Two of the organisations that were subjects of the surveillance were the European Union (EU) and the United Nations (UN).²⁶ Because of the increasing threat of global terrorist attacks, much of it utilising technology, it became necessary for counter-terrorism techniques to be technologically advanced as well, thus providing justification for the “Five Eyes” surveillance.²⁷

In Nigeria, the laws making provision for the lawful utilisation of communications surveillance shows that the State is invested in its deployment. The 2021 budget appropriations indicate that about 4.8bn Naira (approximately \$11.5m) was allocated to “monitor private calls and messages”.²⁸ Recent occurrences in Nigeria have indicated that the government tends towards totalitarianism when it has unrestrained control of communications services networks.²⁹ In June 2021, the Nigerian government

surveillance powers and confirmed the warning in the 1984 novel by George Orwell's a big brother society in which the state watches its citizens.

²⁵ The “Five Eyes” is an alliance of five English speaking countries focused on surveillance intelligence; Nyst “The Five Eyes Fact Sheet”, Privacy International (26 November 2013), <https://privacyinternational.org/news-analysis/1204/five-eyes-fact-sheet> (accessed 2018-10-01); Farrel “History of 5-Eyes-Explainer” (2 December 2013), <https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer> (accessed 2018-10-11); 2014 OHCHR report par [4]. Landau “Making Sense from Snowden” What’s Significant in the NSA Surveillance Revelations”

²⁶ *Ibid.*

²⁷ Dodd “Government’s Defence of Surveillance Unconvincing says ex-watchdog” (2014-06-18) *The Guardian*, <https://www.theguardian.com/world/2014/jun/18/government-surveillance-watchdog-loopholes> (accessed 2019-03-03).

²⁸ Ojo “No to Monitoring of Nigerian’s Communications” (20 October 2021) *Punch Newspaper*, <https://punchng.com/no-to-monitoring-of-nigerians-communications/> (accessed on 2022-02-19); Marczak, Scott-Railton *et al* “Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles” (1 December 2020) *Citizens Lab Research Report No. 133, University of Toronto* <https://tspace.library.utoronto.ca/bitstream/1807/106212/1/Report%23133--runningincircles.pdf> (accessed on 2022-08-01) 9-10; 2017 and 2018 budget allocations signify that N46bn (\$127.6m) and N2.21bn (\$6m) respectively was allocated for communications surveillance; Paradigm Initiative 2018 “The Right to Privacy in the Federal Republic of Nigeria” *Stakeholder Report: Universal Periodic Review 31st Session- Nigeria* 6.

²⁹ Rozen “How Nigeria’s Police used Telecom Surveillance to Lure and Arrest Journalists” (13 February 2020) *Committee to Protect Journalists* <https://cpj.org/2020/02/nigeria-police-telecom-surveillance-lure-arrest-journalists/> (accessed 2020-08-01). In 2020, Rotimi Jolayemi (A Nigerian journalist) was arrested and indicted for spreading WhatsApp messages “causing annoyance, insult, hatred and ill will” to the Minister of Information and Culture – Alhaji Lai Mohammed and charged under for an under section 24(1)(b) of the Cybercrimes (Prohibition, Prevention etc) Act, 2015; In 2018, the Nigerian Minister of Defence – Masur Dan Ali - promises to “support” social media monitoring to apprehend persons distributing messages that are deemed anti-military, anti-government or anti-security; Onwuaso “Paradigm Initiative Challenges Nigerian Government’s Surveillance of Social Media” (29 January 2018)

suspended the use of Twitter when it (Twitter) removed the President's statement "that threatened to punish regional secessionists".³⁰

It has been further reported that the Nigerian government shut down communications service networks in some locations in an effort to slow down Boko-Haram³¹ insurgencies and "protect national security".³² In addition, the State demonstrated a lack of respect for human rights and lives during the "ENDSARS"³³ protest in October 2020 when it ordered the military to shoot at civilians during a peaceful protest at the Lekki toll gate in Lagos, Nigeria. These instances signify that the Nigerian government has a tendency to suppress human rights if it is unrestrained. It is therefore necessary to ensure that the State does not have wide discretionary powers when executing communications surveillance, otherwise, the State has the capacity to use communications surveillance to suppress human rights and erode democracy.³⁴

While counterterrorism measures are necessary in light of the several security issues that face Nigeria, international human rights law must not be ignored when combatting these serious crimes. It is acknowledged that law enforcement agencies require access to information to conduct investigation and that this access will infringe human rights. Indeed, the laws on communications surveillance in Nigeria are heavily tailored towards enabling access to information. A balance between the duty of law

<https://www.nigeriacommunicationsweek.com.ng/paradigm-initiative-challenges-nigerian-governments-surveillance-of-social-media/> (accessed 2022-04-11).

³⁰ Aljazeera News "Nigerian Ends its Twitter Ban after Seven Months" (12 January 2022) <https://www.aljazeera.com/economy/2022/1/12/nigeria-ends-its-twitter-ban-after-seven-months> (accessed on 2022-02-20).

³¹ Boko-Haram is one of the largest Islamist militant groups in Africa and is responsible for several terrorist attacks in Northern Nigeria which includes terrorist attacks on religious groups, bombings, kidnapping school children especially females. Global Conflict Tracker "Boko Haram in Nigeria" (11 March 2022) <https://www.cfr.org/global-conflict-tracker/conflict/boko-haram-nigeria> (accessed on 2022-03-13).

³² Akinkuotu "Banditry: Months after "no fly order", FG shuts down telecom sites in Zamfara" (4 September 2021), <https://punchng.com/banditry-months-after-no-fly-order-fg-shuts-down-telecom-sites-in-zamfara/> (accessed on 2022-02-24).

³³ "On 4 October 2020, a video went viral showing SARS (Special anti-robbery squad) officers dragging two men from a hotel and shooting one of them outside. A few days later, protests erupted across Nigeria. On 11 October, SARS is disbanded. But it was the 5th time since 2015 that the Nigerian authorities pledged to reform the police and disband SARS. Protests continued demanding more than empty promises. On 20 October, the Nigerian army violently repressed a peaceful protest at the Lekki toll gate, shooting at the protesters and killing at least 12 people. Since that day, the Nigerian authorities have tried to cover up the events of the Lekki Toll Gate Shooting. They froze protests leaders' bank accounts and fined news agencies who diffused videos of the shooting." Amnesty International "#ENDSARS Movement: From Twitter to Nigerian Streets" <https://www.amnesty.org/en/latest/campaigns/2021/02/nigeria-end-impunity-for-police-violence-by-sars-endsars/> (accessed on 2022-03-15).

³⁴ 2018 OHCHR report par [6]; *Zakharov v Russia*, App. No. 47143/06, (2015) par [232].

enforcement agencies and the protection of human rights should be the thesis will explore how this can be achieved through adequate safeguards during surveillance. International law sets the global standard for the provision of adequate protection for human rights.³⁵ Ignoring international law on surveillance has led to laws that encourage the continuous, overreaching and unsupervised utilisation of communications surveillance.³⁶

A Nigerian example from 2020 concerns a journalist, Ogundipe, who narrated how the Nigerian Police collaborated with various communications service providers (CSPs), including MTN,³⁷ to acquire his phone records and those of his family and friends.³⁸ Ogundipe's case was one of many in which the Nigerian police were reported to have detained the friends and families of targeted journalists based on the phone records gathered from the communications of these journalists. One such report reads as follows:

"[i]n each case, police used the records to identify people with a relationship to a targeted journalist, detained those people, and then forced them to facilitate the arrest."³⁹

A spokesperson with the Kwara State Police Command later admitted that the police were able to track journalists using "technology through their SIM [cards] that were registered".⁴⁰ These activities demonstrate collaboration between CSPs and the police. This is very worrying as there is no mention made in the reports of a court order authorising the implementation of communications surveillance on the journalists.⁴¹

As discussed throughout the thesis, a major problem with the legal framework of communications surveillance in Nigeria is that it focuses on enabling surveillance

³⁵ De Schutter *International Human Rights Law* 3ed (2019) 8.

³⁶ The ECtHR in *Big Brother Watch v United Kingdom* no.58170/13,62322/14, 24960/15, ECHR (2018) par [445] stated that "[t]he Court has always been acutely conscious of the difficulties faced by States in protecting their populations from terrorist violence, which constitutes, in itself, a grave threat to human rights"; *Othman (Abu Qatada) v United Kingdom*, no. 8139/09, ECHR (2012) par [183]; *Trabelsi v Belgium*, no. 140/10, ECHR (2014) par [117].

³⁷ MTN is a South African multinational mobile telecommunications company operating in many African countries, Nigeria inclusive and Asia.

³⁸ Rozen "How Nigeria's police used telecom surveillance to lure and arrest journalists" (13 February 2020) *Committee to Protect Journalists* <https://cpj.org/2020/02/nigeria-police-telecomsurveillance-lure-arrest-journalists/> (accessed 27 December 2022).

³⁹ *Ibid.*

⁴⁰ *Ibid.*

⁴¹ The discussion in chapters three and five of the thesis indicates the significance of protecting the electronic communications of special categories of people including journalists and legal practitioners in order to safeguard the rights to freedom of expression and fair trial respectively.

rather than protecting human rights.⁴² Consequently, the laws are problem-laden and need reform. The challenge is to ensure a legal framework for communications surveillance in Nigeria which also contain proper safeguards for the protection of human rights and that can withstand rapid changes in ICT.

The next sub-section provides a brief legal background to international, regional and sub-regional law and the South African jurisprudence on the right to privacy and communications surveillance. Thereafter, the problems with the Nigerian legal framework on the right to privacy and communications are addressed. This is followed by the research questions, the justification for choosing South Africa as a comparable foreign law, and the limitations of the study.

1.3 Legal background

1.3.1 International law on the right to privacy and communications surveillance

The thesis proceeds from the standpoint that privacy is a human right because the Nigerian jurisprudence protects privacy in this manner. The thesis also relies on international law as a benchmark upon which laws regulating communications surveillance is evaluated. The International Covenant on Civil and Political rights (ICCPR), 1966; the Convention on the Rights of the Child (CRC), 1989 and the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW), 1990 provide for a right to privacy among other rights.⁴³ Since Nigeria has ratified these treaties, it is obligated to ensure that the domestic laws align with them.

⁴² Another example was reported by Premium Times, a digital news outlet, in which some Nigerian state governors used IMSI catcher provided by a Bulgarian company known as “Circles 3G”, to track the location, text messages and intercept the calls of their opponents. Welekwe “Demystifying Circles 3G mobile phone snooping technology” (18 June 2016) <https://www.premiumtimesng.com/business/business-interviews/205494-demystifying-circles-3g-mobile-phone-snooping-technology-can-protect-privacy-amakiri-welekwe.html?tztc=1> (accessed 2023-01-30).

⁴³ Article 12 of the United Nations Declaration of Human Rights, 1948; Article 17 of the ICCPR; International Covenant on Civil and Political Rights, adopted 16 December 1966, General Assembly Res. 2200 (XXI), U.N. General Assembly Official Record, 21st Session, Supplement No.16, United Nations Doc. A/6316 (1966), 999 U.N.T.S 171 entered into force on 23 March, 1976); United Nations Human Rights Office of the High Commissioner, “International Covenant on Civil and Political Rights” (1996-2018), <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> (accessed 2018-10-01); Article 16 of the Convention on the Right of a Child (CRC), 1989; Document of the OHCHR “Convention on the Right of a Child” <https://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf> (accessed 2018-11-11); The CRC was adopted by the United Nations’ General Assembly Resolution 44/25 of 20 November 1989, it entered into force on 2nd September 1990; Article 14 of the International

Article 17(1) of the ICCPR prohibits the unlawful or arbitrary interference with privacy. The protection on privacy provided in the CRC and the ICRMW are similar to the ICCPR, but they are focused on specific groups, namely children and migrant workers. Whilst these laws are discussed in detail in chapter two, it is important to note here that article 17 of the ICCPR signifies that the right to privacy is not absolute. It may be limited by a lawful and non-arbitrary interference with the right to privacy. The thesis provides a definition to the terms “lawful” and “non-arbitrary” by examining the 1988 UN Human Rights Committee CCPR General Comment No. 16 on article 17 (the General Comment 16), the Siracusa Principles on the limitation and derogation provisions in the ICCPR (Siracusa Principles), Human Rights Council Resolutions, reports of the Office of the High Commissioner on Human Rights (OHCHR), Special Rapporteurs’ reports,⁴⁴ Human Rights Committee (HRC) decisions and resolutions of the Human Rights Commission relating to the right to privacy. These sources indicate that the terms “lawful” and “non-arbitrary” are ascribed a broader meaning than their general meanings, as explained below.

“Lawful” in terms of article 17 in the ICCPR refers to an interference with privacy being regulated by law. However, the existence of a law regulating communications surveillance only fulfils the “lawfulness” requirement if the law complies with the ICCPR. “Non-arbitrariness” in article 17 includes interference with the right to privacy being regulated by a law that is reasonable.⁴⁵ In addition, “non-arbitrariness” refers to the law clearly specifying the circumstances that may prompt interference, the

Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICMW); Document of the OHCHR “International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families” <https://www.ohchr.org/Documents/ProfessionalInterest/cmw.pdf> (accessed 2018-11-11). The ICMW was adopted by the United Nations’ General Assembly Resolution 45/158 of 18 December 1990. It entered in force on 1st July 2003.

⁴⁴ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression by Frank La Rue, A/HRC/23/40, April 17, 2013, https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf par [15] (accessed on 2019-10-21); Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism by Martin Scheinin A/HRC/13/37 [14-19], (28 December 2009).

⁴⁵ Paragraph 4 of the General Comment 16 on article 17; *Hulst v Netherland*, Communication No. U.N.Doc. CCPR/C/82/D/903/1999 (2004) par [7.7]; Annual report of the Office of the High Commissioner for Human Rights (OHCHR) on the Right to Privacy, 28th session, agenda items 2 and 3, A/HRC/28/39, 19 December, 2014; Report of the OHCHR on the Right to Privacy, 32nd session, 8 April 1988, HRI/GEN/1/Rev.9 (I), General comment 16 par [3]; Michael *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) 5.

designated authority to permit interference and a determination on whether to permit interference that is based on a case-by-case basis.

A major issue with article 17 and its interpretation through UN documents is that it is arguably too broad and difficult to apply in a manner that safeguards the right to privacy adequately. For example, in respect of the appointment of a designated authority to permit communications surveillance, many State Parties utilise judicial officers as the designated authority.⁴⁶ Judges may, however, be ill-equipped to handle the complexities that are involved in adjudicating communications surveillance matters in a way that provides adequate protection for human rights.⁴⁷ Another problem is that the compliance with the provisions of the ICCPR may be ineffective if a mere “box-ticking” exercise is followed. Specific guidelines elaborating on the broad guidelines are needed to guide States.

In Nigeria the ICCPR is yet to be domesticated and laws regulating communications surveillance do not comply with the treaty. The laws regulating communications surveillance could therefore be regarded as unlawful and arbitrary. The problems with the laws regulating communications surveillance in Nigeria are discussed in section 4 below and in detail in chapter 4.

1.3.2 Regional laws on the right to privacy and communications surveillance

1.3.2.1 African regional law on the right to privacy and communications surveillance

Nigeria is a Member State of the African Union (AU) and has ratified and domesticated the African Charter on Human and People’s Rights (ACHPR). Consequently, Nigeria is obligated to ensure that her domestic laws align with the ACHPR. Unfortunately, however, the ACHPR does not protect the right to privacy. Nonetheless, the African Court of Human and People’s Rights (ACtHR) can adjudicate on matters relating to

⁴⁶ *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App. No. 62540/00 (2007) par [84]; *Zakharov v Russia* par [263]; S.1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002; S.39(1) of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015.

⁴⁷ In chapter 3 of this thesis, the point is made that judges may be ill-equipped to handle surveillance cases, because unlike the more usual applications before the courts, surveillance matters require the absence of the surveillance subject and are thus peculiar in nature. Presiding officers in surveillance matters must be specially trained to handle the peculiarities of surveillance matters to ensure adequate protection of the human rights of the surveillance subject. In South Africa, for example, judges known as designated judges are appointed to deal with surveillance matters. See Chapter 3, sec.3.8.2.5.1(iv)(b) and sec. 3.8.2.5.2 (ii).

the infringement on the right to privacy, by considering the international law treaties to which the disputing parties are subject. As a result, any suit against Nigeria in respect of violations on the right to privacy will be decided based on the ICCPR, the CRC or the ICRMW, since Nigeria has ratified these treaties.

Although the ACHPR does not provide for a right to privacy, the AU currently recognises privacy as a human right. This position is reflected in the African Charter on the Rights and Welfare of the Child, 1990 (ACRWC)⁴⁸ and the Declaration of Principles on Freedom of Expression and Access to Information, 2019 (the 2019 Declaration). Principle 40(1) of the Declaration provides that “[e]veryone has the right to privacy”. The right to privacy in the Declaration includes the right to protect the “confidentiality” of communications and the protection of personal information.⁴⁹ Any measures to limit the right to privacy must be “justifiable and compatible with international human rights law and standards”.⁵⁰

In line with Principle 40(3), the utilisation of communications surveillance must possess adequate safeguards for the protection of the right to privacy. Principle 41(3) provides for the minimum requirements for laws regulating communications surveillance to be regarded as having adequate safeguards for the right to privacy. These requirements include: pre-authorisation of communications surveillance by “an independent and impartial judicial authority”; procedural safeguards; specificity in terms of the duration, implementation, location and extent of the surveillance; post-surveillance notification to the surveillance subject; “proactive transparency on the nature and scope of its use”; and an effective and independent oversight mechanism.⁵¹ Most of these guidelines, like those provided by international law, are broad and may not be applied in a manner that protects the right to privacy inadequately.

1.3.2.2 European regional law on the right to privacy and communications surveillance

In a bid to find solutions that are more practical for the reform of the legal framework of communications surveillance in Nigeria, the European regional law is very useful and is therefore considered. The European regional law on communications

⁴⁸ Nigeria ratified the ACRWC on the 2 May 2003; Article 10 of the ACRWC; Principle 40 of the 2019 Declaration.

⁴⁹ *Ibid.*

⁵⁰ Principle 40(3) of the 2019 Declaration.

⁵¹ Principle 41(3) of the 2019 Declaration.

surveillance is in an advanced state. This is mostly because the European Court of Human Rights (ECtHR) has tested several domestic laws of its Contracting States.⁵² The ECtHR has developed specific minimum safeguards to guide its Contracting States in regulating their domestic laws on communications surveillance.⁵³ The HRC also refers to the minimum safeguards of the ECtHR in its reports on matters concerning communications surveillance.⁵⁴ The ECtHR's minimum standard on communications surveillance is thus suitable as a benchmark regarding the application of international law to domestic laws.

These minimum safeguards are: the nature of the offence and or activity that can prompt surveillance must be clearly stated; foreseeability namely specificity in respect of the category of people and activities that may prompt surveillance, must be shown; a limitation on the duration of surveillance; and clear and effective procedural guidelines at all stages of surveillance.⁵⁵ The ECtHR has further expounded on the applications of these minimum safeguards in several judgments. Many of the domestic laws scrutinised by the ECtHR in recent judgements had flaws similar to those in the Nigerian laws regulating communications surveillance. The practical application of the minimum safeguards to these domestic laws is a valuable tool to provide recommendations for resolving the problems with Nigeria's laws.

1.3.3 Sub-regional laws on the right to privacy and communications surveillance

1.3.3.1 Economic Community of West African States

Nigeria is a Member State of the Economic Community of West African States (ECOWAS) and has obligations to fulfil the treaties that she has ratified from this coalition. The ECOWAS treaty that recognises a right to privacy is the Supplementary Act on Personal Data Protection within the Economic Community of West African States, 2010 (the Supplementary Act). Article 2 of the Supplementary Act mandates Member States to enact domestic laws that protect personal data. It also provides

⁵² *Association for European Integration and Human Rights and Ekimdzhiiev v Bulgaria; Klass v Germany*, App. No. 5029/71 (1978); *Zakharov v Russia*; *Bigbrother Watch v UK* App. nos. 58170/13, 62322/14, 24960/15 (2018); *Weber and Saravia v Germany*, App. no. 54934/00, 2006-XI ECtHR 1173.

⁵³ *Zakharov v Russia* par [236]; *Huvig v France* 24 April 1990, Series A no. 176 B par [34]; *Kruslin v. France*, 24 April 1990, Series A no. 176A par [35].

⁵⁴ 2018 report par [3].

⁵⁵ *Klass v Germany* par [55]; *Zakharov v Russia* par [233].

guiding principles for the protection of personal data.⁵⁶ The Supplementary Act has no provision relating to the utilisation of communications surveillance. Article 6 also exempts the State from the treaty when it is using personal data for national security and criminal justice procedures. Hence, the Supplementary Act does not regulate the activities of the State in its use of communications surveillance as it falls within the purview of use for national security and criminal justice procedure. The Supplementary Act is therefore not helpful to achieve the aims of this thesis.

1.3.3.2 Southern African Development Community

The Southern African Development Community (SADC) developed a model law on data protection referred to as the SADC Law on Data Protection (SADC Data Protection Law).⁵⁷ The SADC Data Privacy law provides guidelines to Member States on the protection of data privacy. Like the Supplementary Act, the SADC Data Privacy Law also excludes the activities of the State in respect of the protection of national security, defence, public safety and/or the prevention of crime from its provisions. Consequently, the processing of data that occurs during the execution of communications surveillance by the State is exempted from the SADC Data Privacy Law.

1.3.4 The legal framework on the right to privacy and communications surveillance in South Africa

The South African legal framework on the right to privacy and communications surveillance is analysed in this thesis to provide a comparable foreign domestic legal system to guide the reform of Nigeria's law. Although the legal framework on communications surveillance in South Africa is not perfect, recent decisions of the High Court and the Constitutional Court have provided valuable insights on the protection of the right to privacy while executing communications surveillance.⁵⁸ These decisions also reflect many of the principles of international treaties and the

⁵⁶ Article 23 of the ECOWAS Supplementary Act on Personal Data.

⁵⁷ SADC Data Protection Model Law "Establishment of Harmonized Policies for the ICT Market in the ACP Countries" (2013) *Harmonization of ICT Policies in Sub-Saharan Africa*, <https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx> (accessed on 2018-10-26).

⁵⁸ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* 2021 (4) BCLR 349 (CC) par [90] {*AmaBhungane v Minister of Justice* (CC)}; *AmaBhungane v Minister of Justice* 2020 (1) SA 90 (GP) par [27] {*AmaBhungane v Minister of Justice* (GP)}.

recommendations in the UN resolutions on the right to privacy in the digital age. To contextualise the legal framework on communications surveillance in South Africa, it is important to discuss briefly the South African jurisprudence on the right to privacy and its limitations.

1.3.4.1 The constitutional protection of the right to privacy and limitation of rights

In South Africa, the Constitution, the common law and legislation provide for the right to privacy and how it should be limited. Communications surveillance is primarily regulated by the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA).⁵⁹ There are other laws regulating communications surveillance, such as the Criminal Procedure Act (CPA),⁶⁰ the Protection of Personal Information Act (POPIA),⁶¹ the Electronic Communications and Transaction Act (ECTA),⁶² and the Cybercrimes Act.⁶³ These laws defer to the RICA in respect of the regulation of communications surveillance.⁶⁴

Section 14 of the Constitution of the Republic of South Africa, 1996 (the Constitution) provides for the right to privacy. It highlights the privacy of communications as one of the rights protected under the right to privacy.⁶⁵ The constitutional provision for a right to privacy grants individuals a public law remedy in addition to the private law remedies already existing under the common law for invasion of privacy.⁶⁶ The intimate personal sphere of a person is protected to a higher degree compared to when a person moves away from the intimate sphere.⁶⁷

The right to privacy is limited in terms of the limitation clause in section 36 of the Constitution that provides for certain criteria that must be fulfilled for a right to be

⁵⁹ The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

⁶⁰ The Criminal Procedure Act 51 of 1977.

⁶¹ The Protection of Personal Information Act 4 of 2013.

⁶² The Electronic Communications and Transactions Act 25 of 2002.

⁶³ The Cybercrimes Act 19 of 2020.

⁶⁴ S.2 of 70 of 2002.

⁶⁵ S.14(d) of the Constitution; Iles "A Fresh Look at Limitations: Unpacking Section 36" 2007 23 *South African Journal on Human Rights* 77.

⁶⁶ McQuoid-Mason "Invasion of Privacy: Common Law v Constitutional Delict – Does it make a Difference" 2000 *Acta Juridica* 243; Neethling, Potgieter and Roos *Neethling on Personality Rights* 3.

⁶⁷ *Investigating Directorate Serious Economic Offences v Hyundai Motors Distributors (Pty) Ltd* 2000 (10) BCLR 1087 (CC) par [15]; *Bernstein v Bester* 1996 (4) BCLR 449 (CC) par [77]; *NM v Smith* 2007 (5) SA 250 (CC) par [27].

restricted.⁶⁸ First, the limitation envisaged must be authorised by a law of general application. Secondly, the limitation must be “reasonable and justifiable” in an open and democratic society based on human dignity, equality and freedom”.⁶⁹ Thirdly, the factors in section 36(1)(a)-(e) must be considered for the limitation of rights to be reasonably justifiable.

The constitutional limitation clause provides several lessons for Nigeria to emulate. The major lesson is that the limitation of rights must be subjected to a proportionality evaluation between the right to be limited and the aim pursued using the factors provided in section 36(1)(a)-(e). The South African jurisprudence on the right to privacy and the limitation of rights also provide an African example for Nigeria.

1.3.4.2 The common law

Prior to the Constitution, privacy rights were recognised in the South African common law. In South Africa, the protection of privacy as a personality right has its historic basis in the Roman and Roman-Dutch law concept of *iniuria*.⁷⁰ South African case law indicates that *iniuria* is an infringement of a person’s *corpus* (physical and mental integrity), *fama* (good name) or *dignitas*.⁷¹ The wider definition of infringement on *dignitas* was given by Watermeyer J in *O’Keeffe v Argus Printing* as dignity or those rights relating to dignity.⁷² Watermeyer J extended the meaning of *dignitas* to all personality rights that are neither *corpus* nor *fama*.

⁶⁸ McQuoid-Mason 2000 *Acta Juridica* 228; *Case v Minister of Safety and Security* 1996 (3) SA 617 (CC) par [106]. S 36 of the Constitution provides as follows:

“(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including –

- (a) the nature of the right;
- (b) the importance of the purpose of the limitation;
- (c) the nature and extent of the limitation;
- (d) the relation between the limitation and its purpose; and
- (e) less restrictive means to achieve the purpose.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights”

⁶⁹ S.36 (1) of the Constitution; *Bernstein v Bester* 1996 (4) BCLR 449 (CC) par [66].

⁷⁰ Neethling and Potgieter *Law of Delict* 8ed (2020) 8; Loubser and Midgley (eds) *The Law of Delict in South Africa* 3ed (2018) 18.

⁷¹ *NM v Smith* 2007 (5) SA 250 (CC) par [15]; *Bernstein v Bernstein* (1996) (4) BCLR 449 (CC) par [68].

⁷² 1954 (3) All SA 159 (C) 163.

The *actio iniuriarum* under the South African law of delict provides a remedy for wrongful and intentional infringement of personality rights.⁷³ Hence, a *solatium* (satisfaction/solace money) is only provided where an *iniuria* is wrongful and intentional. Preceding the award of satisfaction, the plaintiff must prove the presence of all elements of delict.⁷⁴ The South African common law approach to the protection of the right to privacy shows that there can be a dual protection of the right to privacy and is important for the development of the Nigerian law. The research asks whether the development of a tort of privacy should be considered as a potential remedy for privacy invasions in Nigeria.

1.3.4.3 Legislative framework of communications surveillance in South Africa

Section 1 of the RICA provides a detailed definition of activities that are conducted during surveillance and of persons authorised to implement surveillance. This section provides clarity on issues such as the judicial authority responsible for the granting of a communications surveillance order. It also provides for the designation of the law enforcement officers (LEOs) that can utilise surveillance and for clarity and specificity in respect of the authorised persons to execute communications surveillance. The Act contains a clear definition section, which is an important example for Nigeria to consider because lack of clarity is one of the problems with the Nigerian framework on communications surveillance, as highlighted in section 1.3.5 below.

The RICA further provides for the judicial authorisation of a communications surveillance order.⁷⁵ Chapters 3 and 4 of the RICA provide procedural guidance for the application for a communications surveillance order and the execution of the order. These provisions of the RICA enable transparency about the procedure of communications surveillance in South Africa and about the circumstances that may prompt surveillance. The procedural guidelines in the RICA regarding the authorisation

⁷³ Neethling and Potgieter *Law of Delict* 8ed (2020) 8; Loubser and Midgley (eds) *The Law of Delict in South Africa* 3ed (2018) 18.

⁷⁴ Neethling and Potgieter *Law of Delict* 4; Loubser and Midgley (eds) *The Law of Delict in South Africa* 2ed (2012) 16; This is known as the generalising approach that is used to test whether there is a remedy. The elements of delict that must be proven are conduct, causation, wrongfulness, fault and damage; *Standards Authority of SA* (2005) JOL 15447 (SCA) par [12]; Roehrs "Privacy, HIV/AIDS, and Public Health Interventions" 2009 126 *South African Law Journal* 361; McQuoid-Mason 2002 *Acta Juridica* 228; Neethling and Potgieter *Law of Delict* 80; Neethling and Potgieter *Law of Delict* 45-52; Neethling, Potgieter and Visser *Law of Personality* (2ed) 2005; *Journal* 362; Loubser and Midgley *The Law of Delict in South Africa* 101; *Shabalala v Metrorail* 2008 (3) SA 142 (SCA) par [7].

⁷⁵ S.16 of 70 of 2002.

and execution of communications surveillance reduce the wide discretionary powers available to judicial officers.⁷⁶ It further provides judges with guidance regarding the factors to consider when presiding over a communications surveillance order. These provisions are likely to assist Nigeria as the lack of procedural guidance and the wide discretionary power of judges is another problem with Nigeria's legal framework on communications surveillance. The problems with the Nigerian framework and recommendations for their resolution is discussed in detail in chapters four and five respectively.

1.3.5 The legal framework on the right to privacy and communications surveillance in Nigeria

The right to privacy in Nigeria is protected by the Constitution of the Federal Republic of Nigeria (1999 Nigerian Constitution) and legislation. Various laws that are mainly industry specific regulate the right to privacy as it applies to each specific industry. For example, the Freedom of Information Act, 2011 (FOIA) regulates the processing of personal information regarding a request for disclosure of information held by the State. Other laws include the Child's Right Act, 2003, the National Identity Management Commission Act, 2007 (NIMC Act), the HIV/AIDS anti-discrimination Act, 2014, the Central Bank of Nigeria Act, 2007 (CBN Act), National Health Act, 2014, the Credit Reporting Act, 2017, the Federal Competition and Consumer Protection Act, 2019. These laws regulate the processing of personal information in the various industries and are discussed in detail in chapter four.

Communications surveillance in Nigeria is regulated by the Cybercrimes (Prohibition, Prevention etc.) Act, 2015 (CPPA), the Terrorism (Prevention and Prohibition) Act, 2022 (TPPA), the Nigerian Communications Act, 2007 (NCA) and the Lawful Interception of Communications Regulation, 2019 (LICR).

1.3.5.1 Constitutional protection of the right to privacy and its limitation

Section 37 of the 1999 Nigerian Constitution provides for the right to privacy of Nigerian citizens. It specifically guarantees the protection of the privacy of correspondence, telegraphic communications and telephone conversations. This specific protection of the privacy of communications and correspondence extends to electronic communications including e-mails, phone calls over communications

⁷⁶ Ss.16-19 of 70 of 2002.

networks and instant messaging. The constitutional protection of the right to privacy is, however, flawed as it protects the right to privacy for Nigerian citizens only. Section 37 is thus discriminatory against non-Nigerians.

The right to privacy is limited by section 45(1) of the 1999 Nigerian Constitution that permits any law that is reasonably justifiable in a democratic society to restrict the right. Section 45 provides for legitimate aims for which the right to privacy can be limited and these include the “interest of defence, public safety, public order, public morality or public health or for the purpose of protecting the rights and freedom of other persons.” Unlike the South African Constitution, section 45(1) of the 1999 Nigerian Constitution does not provide for factors that must be considered in evaluating whether a limitation is reasonably justifiable. As a result, Nigerian courts have interpreted section 45(1) in a manner that does not include an evaluation of whether a limitation is reasonably justifiable. That is, the Nigerian Courts are more likely to limit the right to privacy and other rights mentioned in section 45(1) solely on the ground that the limitation serves a legitimate aim.⁷⁷ This interpretation of section 45(1) constitutes a fundamental problem for the protection of the right to privacy (and other rights). Consequently, communications surveillance as a limitation of the right to privacy is likely to be permitted without an evaluation of whether the limiting law is reasonably justifiable. This approach to the interpretation of section 45(1) provides inadequate protection for human rights, **specifically the right to privacy** and is explored throughout the thesis.

1.3.5.2 Legislative framework of communications surveillance in Nigeria

1.3.5.2.1 Nigerian Communications Act

The NCA provides for the legal and regulatory framework of all matters, including the protection of communications privacy, relating to the ICT sector in Nigeria. The NCA also establishes the Nigerian Communications Commission (NCC). Section 71 of the NCA empowers the NCC to make regulations on matters relating to the communications industry in Nigeria. In response to the power to make regulations, the NCC has prepared several regulations to guide the operations of the communications industry in Nigeria. One of the regulations is the Lawful Interception of Communications Regulation, 2019 (LICR) which regulates the execution of

⁷⁷ *Asari Dokubo v Federal Republic of Nigeria* (2007) 12 NWLR (Pt. 1048) 320.

communications surveillance in Nigeria. Other regulations include the Consumer Code of Practice Regulations, 2007 (CCPR) and the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 (RTS regulations).⁷⁸

These are discussed in chapter four, where their constitutionality is explored in detail. Section 146(1) and (2) of the NCA empowers a communications service provider (CSP) to prevent the use of its communications network for criminal purposes and assist “the Commission or other authority” to prevent crimes.⁷⁹ Neither section 146 nor 157 (the section that defines the terms used in the NCA) provide clarity on the specific authorities that are empowered to execute communications surveillance. Hence, all government agencies, for example the Nigerian Television Authority, can assume the position of an authority and approach a communications service provider (CSP) for assistance for the purpose of crime prevention.⁸⁰ Unlike other statutes, such as the Police Act, 1943 that confers law enforcement duties on the police, the NCA does not confer law enforcement duties on the NCC and “other authorities”. Section 146 of the NCA is therefore problematic as being too broad, over-reaching, and lacking clarity.

Section 157 defines an authorised communications surveillance as “interception...permitted under section 148 of this Act”. Section 148(1)(c) provides that in the event of any public emergency or in the interest of public safety, the NCC shall engage in communications surveillance. The definition of an authorised interception of communications as one conducted in line with section 148, which is not subject to other laws, empowers the NCC as the sole authorising body for an interception order. Sections 146, 148 and 157 are therefore conflicting as there are different provisions regarding what constitutes an authorised communications surveillance.

In addition, the definition of an authorised interception is not aligned to definitions in other statutes. It conflicts with the definition of an authorised interception of communications in the TPPA, the CPPA and the LICR that all provide for the authorisation of communications surveillance by a judge. The NCA, by empowering

⁷⁸ Federal Republic of Nigeria Official Gazette No.101, Lagos 7 November 2011, Vol.98, Government Notice No. 229 B1125 – 1134; Federal Republic of Nigeria Official Gazette No.87, Lagos 10 July 2007, Vol.94, Government Notice No.56 B251 – 273.

⁷⁹ S.146 (1) of the NCA; S.157 of the NCA defines a licensee as “a person who either holds an individual licence or undertakes activities which are subject to a class licence granted under this Act.” The licensees of the NCC provide communications services and facilities.

⁸⁰ The Nigerian Television Authority is a television channel owned and controlled by the Federal Government.

the NCC, a parastatal of the State, as the authorising body for a communications surveillance order, deprives the pre-authorisation procedure of its independence. There is, accordingly, a risk that communications surveillance could be ordered at the behest of the State, rather than by an independent authorisation body as required by international and African regional law.

Furthermore, section 148 provides that communications surveillance is permissible only in “the occurrence of a public emergency or in the interest of public safety”. Where there is no public emergency or a threat to public safety, the NCC cannot order its licensees to execute authorised communications surveillance. Since the NCC is the sole authorising body for communications surveillance under the NCA, it is precluded from authorising surveillance where surveillance is required for situations that are neither a “public emergency nor in the interest of public safety”. Section 45 of the 1999 Nigerian Constitution provides for broader aims for which the right to privacy can be limited and these are the interest of defence, public safety, public order, public morality, public health and the preservation of the rights and freedom of others. The NCA therefore does not align with the 1999 Nigerian Constitution in respect of the legitimate aims for which communications surveillance can be executed.

Lastly, the NCA does not provide any procedural guidance for the execution of communications surveillance. The State has a wide discretion to utilise surveillance and the information obtained from such surveillance as it wishes. The right to privacy of a subject of surveillance is therefore not protected under the NCA. There is also no avenue for redress for a surveillance subject under the NCA.

1.3.5.2.2 Lawful Interception of Communications Regulation

The LICR is the only law that has as its main objective the regulation of communications surveillance in Nigeria.⁸¹ However, it is a subordinate law and inferior in hierarchy to the CPPA and the TPPA. In the event of a conflict between the LICR and the other statutes, the CPPA and the TPPA will prevail. The LICR, is therefore, ineffective as the principal law on communications surveillance in Nigeria.

The LICR provides for judicial authorisation of a communications surveillance order.⁸² Judicial officers are, however, not given guidance regarding the factors to consider

⁸¹ Regulation 1 of the LICR.

⁸² Regulation 7(2) of the LICR.

when authorising a communications surveillance. The LICR does not mandate LEOs to disclose full information regarding the application for a communications surveillance nor does it empower the judges to request additional information. A communications surveillance order is authorised, based on the information provided in the application. The problem is that the information may be false. There is also no prohibition of the execution of a communications surveillance order without judicial authorisation.⁸³ As a result, LEOs may circumvent the judicial authorisation of communications surveillance with impunity. The LICR is therefore prone to abuse and provides inadequate safeguards for the right to privacy.

Communications surveillance is used for law enforcement duties that involves the investigation and prevention of criminal activities. Thus, the institution formulating the law that regulates communications surveillance must be constitutionally empowered to make laws in respect of law enforcement duties. This is because law enforcement is in the exclusive legislative list in the 1999 Nigerian Constitution. The NCA, and by extension the NCC, does not have the constitutional mandate to regulate law enforcement duties. The LICR thus overreaches the law-making powers conferred on the NCC. Furthermore, the LICR extends the ambit of the legitimate aims permissible in section 45(1) of the 1999 Nigerian Constitution by providing for additional aims for which communications surveillance may be executed. These additional aims include “protecting and safeguarding the economic well-being of Nigerians”, “in the interest of public emergency...” and “giving effect to international mutual assistance agreements”.⁸⁴ Consequently, the LICR conflicts with section 45 of 1999 Nigerian Constitution. Ultimately, the LICR is flawed, prone to abuse and provides inadequate safeguards for the right to privacy.

1.3.5.2.3 Cybercrimes (Prohibition, Prevention, Etc) Act

The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 (CPPA) was enacted to prohibit, prevent, detect, investigate, prosecute and respond to cybercrimes and matters related thereto.⁸⁵ It classifies the unlawful interception of communications and the unlawful access to a computer as a cybercrime.⁸⁶ In respect of communications

⁸³ Regulation 4 of the LICR.

⁸⁴ Regulation 7(3)(c), (d) and (e) of the LICR.

⁸⁵ S.1 of the CPPA.

⁸⁶ Ss.5 – 16 of the CPPA.

surveillance, section 38(1) of the CPPA provides for the retention of traffic data (metadata) and subscriber information for a period of two years. However, any law enforcement agency (LEA) and/or “the relevant authority [who is] for the time being, responsible for the regulation of communication services in Nigeria [the NCC]” may request that the service provider preserve or retain any metadata, subscriber information and content or non-content data.⁸⁷ It signifies that judicial authorisation is not required for the retention of metadata. The CPPA disregards the requirement for an independent authorisation body for the utilisation of communications surveillance. This approach reflects an outdated position in light of ICT inventions, namely that the acquisition of metadata is not as intrusive as the interception of communications.⁸⁸ The CPPA, therefore, does not therefore provide adequate safeguards for the right to privacy.

Section 39 of the CPPA provides for the judicial authorisation of communications surveillance where there are reasonable grounds to believe that a crime has been or will be committed. Although the objective of the CPPA is to create, prevent and punish the offence of cybercrime, section 39 extends the utilisation of communications surveillance to all crimes. By so doing, the CPPA extends its ambit to matters other than cybercrimes. Consequently, LEOs can apply for a communications surveillance order under the CPPA for the investigation and/or criminal proceedings of both minor and serious crimes. This negates the principle of necessity for the limitation of rights under the ICCPR rights. This is because section 39 of the CPPA does not restrict the granting of a communications surveillance order to circumstances where it is necessary.

1.3.5.2.4 Terrorism (Prevention and Prohibition) Act, 2022 (TPPA)

The TPPA of Nigeria was enacted to create offences relating to terrorism.⁸⁹ The TPPA prohibits terrorism, provides steps to ban an organisation conducting terrorist related activities and provides punishment for various acts of terrorism.⁹⁰ Section 68(1) of the TPPA permits LEOs to execute communications surveillance when investigating terrorism related crimes and with judicial authorisation.

⁸⁷ S.38 (2) of the CPPA.

⁸⁸ 2014 OHCHR report par [19].

⁸⁹ S.98 of the TPPA repealed the Terrorism (Prevention) Act, No. 10 of 2011.

⁹⁰ S.2 of the TPPA.

The TPPA provides for two levels of authorisation that is, approval by the Coordinator of National Security Adviser (NSA) and a judge. While this appears to be an appropriate provision for the requirement for oversight for communications surveillance, the NSA is an appointee of the President and not independent. Section 68 is the only provision providing for communications surveillance in the TPPA and its purpose is to enable the LEOs to execute communications surveillance in relation to terrorism-related crimes. Thus, the TPPA does not provide procedural guidelines for communications surveillance nor does it provide any other protection for the right to privacy aside from judicial authorisation of a communications surveillance order.⁹¹ The scope of the TPPA is therefore too narrow to serve as the primary law on communications surveillance in Nigeria.

1.3.5.3 Summary of the problems with the Nigerian legislative framework on communications surveillance.

It is clear that there are a number of problematic areas with the legal framework for communications surveillance in Nigeria. Four major thematic themes can be identified, although the problems do tend to overlap. These are:

- The lack of a single, comprehensive, and clear statute regulating communication surveillance, which encompasses sub-themes such as conflicting terminology, overreach and a legitimate and communications surveillance purpose, and lack of foreseeability (meaning that the law is not clear and thus people do not know what is expected of them);
- Ineffective procedural guidelines at all stages of communications surveillance, which includes overbroad powers for intercepting authorities, a broad power to authorise additional warrants and inadequate protection of personal information and the right to a fair hearing;
- Ineffective oversight mechanisms for communications surveillance, which includes an analysis of the role of judges in the process; and
- The lack of an effective avenue for legal redress for the communications subject which involves the lack of post-surveillance notification to the surveillance subject and very few avenues for legal redress after the surveillance has been conducted.

⁹¹ S.68(2) of the TPPA.

Each of these themes is now briefly introduced. Chapter four contains a more detailed analysis of the various challenges and the specific laws in issue.

1.3.5.3.1 Lack of a comprehensive statute

A comprehensive statute regulating communications surveillance in Nigeria has not been enacted. Other statutes, namely the CPPA, TPPA and NCA, contain provisions addressing communications surveillance, but these provisions are merely incidental to their main objectives. As a result, there are many conflicting provisions between the statutes. Although, the LICR does focus on the regulation of communications surveillance, it is a subsidiary law and is lower in hierarchy to the TPPA, CPPA and the NCA. It will be shown that the LICR is, therefore, not suitable to serve as the primary law dealing with communications surveillance in Nigeria. The consequence is a number of related problems such as:

- Conflicting definitions for important terms including the meaning of unlawful interception communication itself;
- A tendency of the LICR to overreach its empowering law, that is the NCA;
- Overreach into the exclusive authority of the legislature to enact laws in respect of law enforcement in Nigeria; and
- An unclear objective underpinning the regulation of the interception of communications, which infringes the 1999 Nigerian Constitution.

1.3.5.3.2 Ineffective procedural and inadequate guidelines at all stages of communications surveillance

The Nigerian legal framework on communications surveillance lacks effective procedural guidelines at all stages. There are three stages namely - authorisation, execution and post-surveillance. Although the CPPA and the LICR provide procedural guidelines at the pre-authorisation stage, these lack detail and do not guide presiding officers adequately when considering an application for a communications surveillance. The result is a wide discretionary power. Another problem is that presiding officers are not required to provide reasons for their rulings. The authorisation stage therefore lacks transparency and is prone to abuse. None of the laws provide any procedural guidelines for the execution and post-surveillance stages. Thus, under this theme, the following problems are addressed: the broad powers of law enforcement agencies; the reality of an optional warrant for an application for the

interception of communications; inadequate protection of personal information; and the right to fair hearing.

1.3.5.3.3 Ineffective oversight mechanisms for communications surveillance

The problem described in the heading also impacts on the effectiveness of the oversight mechanisms and bodies who should monitor the grant of a surveillance warrant. Although the judiciary is independent, the laws do not stipulate that all relevant information must be placed before a judge who is required to decide whether a communications surveillance order should be granted. The result is that the judge is unable to make an informed decision and must rely only on the LEOs application, made *ex parte* and which tends to be one-sided. This state of affairs impacts negatively on the human rights of the surveillance subject.

1.3.5.3.4 An effective avenue for redress

The final theme addresses the fact that the surveillance subject has no recourse in the event of an unlawful execution of communications surveillance because he or she is not notified of the surveillance after its completion. In the unlikely event that surveillance subjects become aware of the surveillance, they are only entitled to claim constitutional damages, with stringent conditions to be fulfilled for a successful claim.⁹² Furthermore, such damages are usually granted only as a punitive measure.⁹³ There is therefore a need for the development of the law to provide for post-surveillance notification and effective avenues for legal redress.

1.4 Aims and objectives of the study

The objective of this study is to analyse how communications surveillance in Nigeria should be better regulated so that the right to privacy is not unlawfully and arbitrarily infringed. It further aims to provide recommendations in order to achieve a balance between the need for the State to utilise communications surveillance and the duty to protect human rights adequately in the process.

The study recommends reform to the current legal framework of communications surveillance in Nigeria and also advocates for an interpretation of section 45(1) that ensures that the rights listed in that section are not limited in a manner which

⁹² S 35(6) of the 1999 Nigerian Constitution; *Enanuga v Sampson* (2012) LPELR-8487 (CA) 20.
⁹³ *Ibid.*

unjustifiably infringes the rights. It will be shown that a human-rights based approach to communications surveillance needs a dual approach: tightly drafted and clear laws and a limitation clause which is designed to protect rights optimally.

To achieve these objectives, the study explores international, regional and sub-regional laws on the right to privacy and communications surveillance in order to determine the international standard. Thereafter, the study examines South Africa's legal framework on the right to privacy and communications surveillance to extract valuable lessons for the proposed reforms in Nigeria. The study further analyses the legal framework on communications surveillance in Nigeria with a view to providing a detailed exposition of the problems with the Nigerian framework. Recommendations for rectifying the problems are then provided.

1.5 Research questions

The main question this research addresses is: how can the Nigerian legislative framework on communications surveillance be reformed to conform with international standards? To answer the main question, the following questions are considered:

Firstly, what is the importance of the right to communications privacy in the digital age and what is the impact of unlawful and arbitrary laws on communications surveillance in a democracy?

Secondly, what are the existing international, regional and sub-regional standards for legislation on communications surveillance?

Thirdly, how does South Africa's communications surveillance framework operate and is this regime lawful and non-arbitrary? What can Nigeria learn from South Africa's jurisprudence on the right to privacy and communications surveillance?

Fourthly, given that several problems have been identified with the Nigerian legal framework on communications surveillance and the constitutional limitational clause (section 45 of the 1999 Constitution), what are the legal reforms that are necessary to ensure a communications surveillance regime that adequately protects the right to privacy?

Lastly, what recommendations can be proposed to rectify the problems associated with the legal framework of communications surveillance in Nigeria?

1.6 Methodology

The research employs a desktop method in collating all information required to answer the research questions. This method includes the use of primary and secondary sources of information. The primary sources are international, regional and sub-regional instruments, constitutional provisions, national legislation and case law. The secondary sources are textbooks, journal articles, published and unpublished dissertations, preparatory works of legislation, conference and seminar papers. A rights-based approach to communications surveillance is the methodology used for this thesis.

The study further embarks on comparative legal study on the jurisprudence of the right to privacy between South Africa and Nigeria. The reasons for choosing South Africa's privacy and communications surveillance laws for the purpose of comparison with Nigeria are as follows: Firstly, South Africa is an African country and shares common problems with Nigeria that are Africa specific. South Africa has a rich legal scholarship on the protection of privacy and its law on communications surveillances provide valuable practical remedies. This jurisprudence is capable of guiding reform in Nigeria. Moreover, South Africa's law on communications surveillance has been tested judicially and the decisions of both the High Court and the Constitutional Court in this regard are useful in making practical recommendations for Nigeria's framework.

Secondly, both Nigeria and South Africa have ratified the same international and regional treaties on privacy. These are the ICCPR, CRC, ICMW and the ACHR. Both countries' domestic legislation on the right to privacy should therefore reflect the principles of these treaties. Furthermore, the right to privacy is constitutionally protected in both South Africa and Nigeria and justiciable in both countries.

Lastly, South Africa has had over 20 years' experience in legislating communications surveillance. The first legislation was the Interception and Monitoring Prohibition Act, 1992.⁹⁴ The Act was repealed in 2002 and replaced by the RICA. There have subsequently been two amendments to RICA in 2008 and 2010. These amendments suggest that South Africa is continually improving her legislation on communications surveillance, thus making South African law a suitable comparator for Nigeria.

⁹⁴ The repealed Interception and Monitoring Prohibiting Act 127 of 1992.

1.7 Limitations of the study

The study investigates the extent to which Nigeria's legislation on communications surveillance is non-compliant with international standards, with a view to recommending reforms. It analyses the protection of communications privacy and legislation on communications surveillance in international, regional and sub-regional treaties. Other aspects of privacy, such as bodily and territorial privacy, are excluded from this study. Furthermore, data privacy is examined only as it relates to communications privacy and communications surveillance. Thus, statutes that provide for other aspects of privacy and not communications surveillance are not discussed in detail.

Although the right to privacy is the primary right affected by communications surveillance, there are other rights affected by communications surveillance, namely freedom of expression, the right to a fair hearing and fair trial, and the right of access to courts. However, this study focuses mainly on the right to privacy and discusses the impact of communications surveillance on other rights only as they relate to the protection of the right to privacy. Consequently, an in-depth study of the impact of communications surveillance on the rights to freedom of expression, a fair hearing, a fair trial and access to courts is excluded.

In addition, the study focuses on internal surveillance by the State, that is surveillance occurring within the borders of a country, hence external surveillance (extraterritorial surveillance) is excluded from this study. Mass/bulk surveillance is also excluded as the study focuses on targeted communications surveillance only.

The study of surveillance conducted by private sector was further excluded from this study because its justification is based on the appropriation of data aggregation and mining for economic rights. This falls within the category of data privacy and relates to the horizontal application of human rights, that is between the private sector and the surveillance subject.⁹⁵ The focus in this study is communications surveillance conducted by the State.

⁹⁵ Cockfield "Who Watches the Watcher? A Law and Technology Perspective on Government and Private and Sector Surveillance" 2003 29 *Queen's Law Journal* 374.

1.8 Significance of the Study

As indicated throughout the study, the protection of the right to privacy when communications surveillance is used is an emerging area of law. It comprises an analysis of the permissible limitations to the right to privacy in the digital age. Countries such as Germany, the UK and the US are developing standards that ensure that there is a balance between the protection of the right to privacy and the utilisation of surveillance. The standards are reflected in the European regional law on communications surveillance, which is discussed in chapter two. In Nigeria, however, there is little research addressing the question of how the law should respond to communications surveillance in the digital age. Prior studies have mainly addressed the question of data privacy.⁹⁶ The focus of this study, however, is on communications surveillance. The study is therefore original and seeks to fill the gap in the existing knowledge by making recommendations for the reform of the legal framework of communications surveillance in Nigeria by protecting the human rights of surveillance subjects in circumstances where law enforcement officers need to access communications surveillance content/metadata.

1.9 Chapter summary

Chapter one introduces the thesis by providing a legal background to the study, stating the research problem to be addressed, the methodology to be utilised, the limitation of the study and the structure of the chapters.

In chapter two an in-depth analysis of international, regional and sub-regional treaties on the right to privacy and communications surveillance is undertaken. The purpose of the chapter is to investigate the international standards for domestic laws on communications surveillance.

Chapter three examines the legal protection of privacy and the communications surveillance regime in South Africa. The chapter furthermore explores the alignment

⁹⁶ Abdulrauf and Daibu "New Technologies and the Right to Privacy in Nigeria: Evaluating the Tension between Traditional and Modern Conceptions" 2016 7 2016 7 *NAUJILJ* 113; Abdulrauf "The Challenges for the Rule of Law Posed by the Increasing Use of Electronic Surveillance in Sub-Saharan Africa" 2018 18 *AHRLJ* 369; Abdulrauf *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* (doctoral thesis 2015); Ilori "Framing a Human Rights Approach to Communications Surveillance Law through the African Human Rights System in Nigeria, South Africa, Uganda" 2021 *African Human Rights Year Book* 134.

of the laws regulating communications surveillance in South Africa with the Constitution and international law. Thereafter, the chapter concludes by collating good examples for Nigeria to emulate and potential loopholes to avoid.

Chapter four examines the protection available for privacy in Nigeria and analyses whether the laws regulating communications surveillance provide adequate protection for the right to privacy. The chapter includes a discussion of the problematic constitutional provision which permits the limitation of rights, including the right to privacy, and the weak legal framework for communications surveillance. It expands on the four thematic problem areas with the existing laws as highlighted in 1.3.5.3 above and does so by addressing the various communications surveillance laws. The chapter also reveals the need for a reform.

Chapter five recommends a right-based approach to the communications surveillance regime in Nigeria. First, it provides possible solutions to the problem that occurs as a result of the constitutional limitation of the right to privacy. Thereafter, the chapter provides recommendations for the enactment of a new communications surveillance statute that will protect human rights adequately. It draws lessons from international law, regional law and South Africa.

Chapter six concludes the thesis by providing answers to the research questions and summarising the recommendations for Nigeria.

CHAPTER TWO

INTERNATIONAL, REGIONAL AND SUB-REGIONAL LAW ON THE REGULATION OF COMMUNICATIONS SURVEILLANCE

2.1 Introduction

The purpose of this chapter is to determine the standard in the international, African regional and sub-regional laws for the permissible limitation on the right to privacy. Determining the international standard will help to delineate the minimum requirements for legislation on communications surveillance. For this reason, the chapter commences with an analysis of international law on the right to privacy. It will consider the manner in which the right to privacy can be limited and analyse specific provisions on interference with privacy in international law. Thereafter, the chapter examines regional and African sub-regional laws on the right to privacy with a view to determining whether there is any statutory guidance on the regulation of communications surveillance.

As discussed below,⁹⁷ the African Charter on Human and Peoples Rights does not provide for the right to privacy. The African sub-regional laws are also silent on communications surveillance, save for a few provisions on metadata, that are inferred from the Southern African Development Community (SADC) and the Economic Community of West African States (ECOWAS) model laws on the protection of personal data. For this reason, the chapter will examine European regional law in more detail and the minimum requirement for the regulation of communications surveillance which have been developed by the European Court of Human Rights (ECtHR).

It will be shown that the United Nations Human Rights Committee (HRC) has referred to the judgments of the ECtHR in its reports on the right to privacy in the digital age. Also, the HRC has relied on the decisions of the ECtHR for its decisions on communications surveillance. Therefore, the decisions of the ECtHR on interference with privacy have persuasive influence on the decisions of the HRC.

The findings in this chapter will be used to guide the proposed reforms for the Nigerian legal framework on communications surveillance.

⁹⁷ Chapter 2, sec. 2.3.1.

2.2 International law on the right to privacy

International treaties do not impose obligations on Member States to incorporate the specific wording of their texts into domestic legislation.⁹⁸ However, the legislation of Member States must reflect their obligations in terms of international law, so that all beneficiaries and parties to the agreement can mutually benefit from the treaties.⁹⁹ Treaties are clear sources of international law because their provisions define the obligations of the Member States that ratify them. Other sources of international law include declarations, resolutions, General Comments, judicial precedent, state practice and teachings of respected academics.¹⁰⁰

Unlike treaties, these other sources do not have binding force. They merely constitute rules of practice by States and are persuasive sources of international law in international courts.¹⁰¹ In this thesis, recognition is given to this delineation and the principles of international law on the right to privacy and its limitations is gathered from treaties, declarations, resolutions, explanatory documents, the HRC's reports and decisions of international courts. It is important to note that international law should provide general rules that will guide Member States in the enactment of their domestic laws. These general rules should provide clarity and definite guidance to Member States in the enactment of their laws. Each Member State then has the sovereignty to determine methods of implementation of international law.¹⁰²

The discussion in this chapter will commence with the Universal Declaration of Human Rights (UDHR), a UN declaratory document, and move to binding treaties, including the International Covenant on Civil and Political Rights (ICCPR), the Convention on

⁹⁸ The two routes for the incorporation of treaties in domestic legislation are the monist and dualist approaches. The monist view holds the theory that treaties should be adopted directly as part of domestic legislation, while the dualist theory supports the view that treaties must be enacted as law before they are recognised as a domestic law; Coyle "Incorporative Statutes and the Borrowed Treaty Rule" 2010 50 *Virginia Journal of International Law* 655, 656.

⁹⁹ Brewster "The Domestic Origins of International Agreements 2004 44 *Virginia Journal of International Law* 501, 540; Hathaway "Do Human Rights Treaties Make a Difference?" 2002 111 *Yale Law Journal* 1935-1940.

¹⁰⁰ Thirlway *Sources of International Law* 2ed (2019) 95.

¹⁰¹ D'Aspremont "The Idea of 'Rules' in the Sources of International Law" 2013 84 *British Yearbook of International Law* 105; Shaw *International law* 9ed (2021) 59; ICJ's Advisory Opinion Concerning *Legal Consequences of the Construction of a Wall in the Preoccupied Palestinian Territory*, ICJ reports (2004) 136, 171; Fitzmaurice "History of Article 38 of the Statute of ICJ" in Besson and D' Aspremont (eds) *The Oxford Handbook of the Sources of International Law* (2017) 188.

¹⁰² Diggelmann and Cleis "How the Right to Privacy Became a Human Right" 2014 14 *Human Rights Law Review* 451.

the Rights of the Child (CRC), the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW), all of which are UN treaties with provisions on the right to privacy.¹⁰³ In addition, the Siracusa Principles on the limitation and derogation provisions in the ICCPR (Siracusa Principles) are discussed in section 2.1.2.2 below as a definitional document to the ICCPR.¹⁰⁴ Although the Siracusa Principles document is neither a treaty nor a resolution and therefore not binding on Member States, it is a useful explanatory document on terms that are used in the ICCPR and can therefore guide state practices.

2.2.1 The Universal Declaration of Human Rights

The UDHR was adopted by the United Nations in 1948 and serves as a template for international standards on human rights globally.¹⁰⁵ The UDHR, being a statement of principles, provides a standard by which States may be assessed on their obligation to protect human rights.¹⁰⁶ The UDHR is a declaration and lacks the binding force of a treaty. However, subsequent UN treaties on human rights such as the ICCPR, the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the CRC, reflect the principles contained in the UDHR.¹⁰⁷ The Siracusa Principles highlight the importance of the UDHR by defining a democratic society as one that incorporates and respects the rights set out in the UDHR and the United Nations Charter.¹⁰⁸ “[T]he

¹⁰³ UDHR, 10 December 1948, GA Res. 217 A (III); ICCPR, 16 December 1966, 999 UNTS, 171; CRC, 20 November 1989, 1577 UNTS, 3; International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, 18 December 1990, 2220 UNTS 3 (entered into force 1 July 2003); Barbaro “Government Interference with the Right to Privacy: Is the Right to Privacy an Endangered Animal?” 2017 6 *Canadian Journal of Human Rights* 142.

¹⁰⁴ E/CN.4/1985/4, annex; Siracusa Principles (April, 1985), <https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf> (accessed 2019-06-10); The deliberations in the Siracusa Principles on necessity and proportionality were adopted by the Human Rights Committee in their General Comment 14 paragraphs 28 and 29; Silva and Maxwell “Commentary: Limiting Rights and Freedoms in the Context of Ebola and Other Public Health Emergencies: How the Principle of Reciprocity Can Enrich the Application of the Siracusa Principles” (2 June 2015) *Health and Human Rights*, <https://www.hhrjournal.org/2015/06/commentary-limiting-rights-and-freedoms-in-the-context-of-ebola-and-other-public-health-emergencies-how-the-principle-of-reciprocity-can-enrich-the-application-of-the-siracusa-principles/> (accessed 2021-02-08).

¹⁰⁵ Shaw *International Law* (2021) 33.

¹⁰⁶ Udombana “Mission Accomplished? An Impact Assessment of the UDHR in Africa” 2008 30 *Hamline Journal of Public Law and Policy* 337; Engle “Universal Human Rights: A Generational History” 2006 12 *Annual Survey International and Comparative Law* 219, 220; De Baets “The Impact of the “Universal Declaration of Human Rights” on the Study of History” 2009 48 *History and Theory* 20-21.

¹⁰⁷ ICESCR, 16 December 1966, 993 UNTS, 3.

¹⁰⁸ Siracusa Principles par [B-21].

UDHR remains in and of itself something of crucial educational importance and a vital foundation of the global ethic of human rights.”¹⁰⁹

Nigeria is a Member State of the United Nations. In her National Action Plan for the Promotion and Protection of Human Rights, Nigeria specifically recognises the UDHR as one of the international instruments that she is obligated to fulfil.¹¹⁰ Nigeria’s provisions on human rights must therefore reflect the principles of the UDHR and other human rights treaties that she has ratified. Although the UDHR is not adopted as law in Nigeria, Nigerian courts refer to it in their decisions on fundamental human rights.¹¹¹ This is because the preamble to the Fundamental Rights (Enforcement) Procedure (FREP) Rules lists the UDHR as one of the international bills of rights that shall influence the court’s decisions on fundamental human rights.¹¹²

The UDHR prohibits arbitrary interference with privacy and correspondence. Article 12 of the UDHR provides as follows:

“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.”

Article 12 of the UDHR provides for a right to the protection of the law against arbitrary interference of privacy and correspondence from others. The protection of the law can occur before an infringement of the right to privacy by setting up safeguards against such infringement. Also, protection of the law can occur after an infringement of article 12 of the UDHR by ensuring that there are appropriate remedies to compensate for infringement of rights. Consequently, article 12 creates three requirements for the protection of the right to privacy, home, family or correspondence. Firstly, interference with privacy, family, home or correspondence must be non-arbitrary.¹¹³ Secondly, there must be safeguards against arbitrary interference of privacy, home, family or

¹⁰⁹ Brown (ed) *A report by the Global Citizenship Commission - The Universal Declaration of Human Rights in the 21st Century: A Living Document in a Changing World* (2016) 59.

¹¹⁰ The NAP is Nigeria’s response to the recommendation of the Vienna Declaration and Programme of Action, adopted at the World Conference on Human Rights in Vienna Austria in 1993.

¹¹¹ *Udo v Robson* (2018) LPELR-45183 (CA) 13-17; *Tolani v Kwara State Judicial Service Commission* (2009) LPELR- 8375 (CA) 33; *Kim v State* (1992) LPELR-1691 (SC) 12; *United Bank for Africa v Unisaes* (2014) LPELR-24283 (CA) 27; *Omonyahuy v The Inspector-General of Police* (2015) LPELR-25581 (CA) 52-56.

¹¹² Preamble 3(b)(ii) of the Fundamental Rights (Enforcement) Procedure Rules of Nigeria, 2009.

¹¹³ Article 12 of the UDHR.

correspondence.¹¹⁴ Lastly, there must be adequate redress for arbitrary interference with privacy, family, home or correspondence.¹¹⁵ The UDHR, does not, however, define the term “arbitrary”.

Article 12 of the UDHR protects privacy of one’s correspondence against arbitrary interference, thereby signifying that the right is not absolute. Article 12 recognises the need for interference with privacy, family, home or correspondence where necessary, but it does not include a built-in requirement for the permissible limitation of the right. Article 29, however, provides for a general limitation clause for UDHR rights as follows:

Article 12 of the UDHR does not provide a built-in requirement for the permissible limitation of the right to privacy and correspondence. However, article 29 provides for a general limitation clause for all the rights in the UDHR. Article 29 of the UDHR provides for the limitation of the rights in the UDHR as follows:

- “(1) Everyone has duties to the community in which alone the free and full development of his personality is possible.
- (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.
- (3) These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.”

Article 29(2) of the UDHR provides that limitation of the rights in the UDHR, including the right protected by article 12, must be limited by law. This means that any interference with privacy, home, family and correspondence must be lawfully regulated. This sub-article sets out the manner and circumstances in which human rights may be limited. Limiting laws must be enacted for the purpose of securing the rights and freedoms of others and of meeting the requirements of morality, public order and the general welfare in a democratic society. Any law limiting privacy and/or correspondence that is not for the purposes set out in article 29(2) of the UDHR is arbitrary. The UDHR does not specify whether the law must be a statute. As a result, Member States have the flexibility to determine the mode of law for which interference

¹¹⁴ *Ibid*; The protection of the law against arbitrary interference or attacks to privacy, home, family and correspondence implies that the law must be adequate to safeguard persons against arbitrary interference.

¹¹⁵ Article 8 of the UDHR provides as follows: “Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.”

with privacy will be regulated. It follows that as communications surveillance is a limitation of the right to privacy, it must be regulated by law and be executed for the purposes set out in article 29(2) of the UDHR.

The clauses in article 29(2) of the UDHR, that is: “provided by law”, “just requirement of morals”, “public order”, “general welfare in a democratic society” are mutually inclusive because of the use of “and” rather than “or”. Like “arbitrariness”, these terms are not defined. This creates some difficulties and it has been argued that the provisions of the UDHR are abstract.¹¹⁶ Fortunately, the article 29(2) terms are defined in the Siracusa Principles and discussed in section 2.2.2.2 below.¹¹⁷

2.2.2. International Covenant on Civil and Political Rights

The ICCPR provides for the protection of human rights and is legally binding on 167 States.¹¹⁸ The Office of the UN High Commissioner for Human Rights (OHCHR) describes the ICCPR as a treaty that elaborates on the civil and political rights set out in the UDHR.¹¹⁹ The ICCPR is the only legally binding international treaty protecting the right to privacy that applies to everyone within the territory of Member States of the UN and is the most important treaty on the right to privacy.¹²⁰ As discussed below, other UN instruments protecting the right to privacy address specific categories of persons such as children.

¹¹⁶ Cho “Rethinking Democracy and Human Rights Education on the Seventieth Anniversary of the Universal Declaration of Human Rights” 2019 20 *Asia Pacific Education Review* 173.

¹¹⁷ Siracusa Principles par [B19-35].

¹¹⁸ Nigeria became a Member State of the United Nations on the 7 October 1960 while South Africa became a Member State on the 7th November 1945; United Nations, “Member States”, <https://www.un.org/en/about-us/member-states> (accessed on 2018-12-7).

¹¹⁹ Shope “The Adoption and Function of International Instruments: Thoughts on Taiwan’s Enactment of the Act to Implement the ICCPR AND the ICESCR” 2012 22 *Indiana International & Comparative Law Review* 163; United Nations Factsheet No. 30, OHCHR, the UN Human Rights Treaty System: An Introduction to the Core Human Rights Treaties and the Treaty Bodies, <https://www.ohchr.org/sites/default/files/Documents/Publications/FactSheet30Rev1.pdf> (accessed 2018-12-07).

¹²⁰ The CRC and the ICRMW are UN treaties that also provide for the right to privacy, however their provisions relate to the protection of the rights of children and migrant workers respectively; Zilli “Approaching Extraterritoriality Debate: The Human Rights Committee, the U.S. and the ICCPR” 2011 9 *Santa Clara International Law Journal* 401; Rakower “Blurred Line: Zooming in on Google Street View and the Global Right to Privacy” 2011 37 *Brook Journal of International Law* 335; Scheinin, report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Human Rights Council, 13th Session, Supp. No.3, UN Doc A/HRC/13/37 (2006) 6; Tomuschat “International Covenant on Civil and Political Rights”) http://legal.un.org/avl/pdf/ha/iccpr/iccpr_e.pdf (accessed on 2018-10-01) 1.

Article 17 of the ICCPR obligates Member States to protect the right to privacy. It provides as follows:

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

The protection offered in terms of article 17(1) of the ICCPR, like the UDHR, protects not only privacy, but also family, home, correspondence, reputation and honour. The direct inclusion of the lawfulness of interference with privacy in article 17(1) of the ICCPR introduces four categories of protection when compared to the three in the UDHR. The first is the protection against unlawful interference with privacy, family, home or correspondence. The second category is the protection against the arbitrariness of any interference with privacy, family, home or correspondence. The third category refers to unlawful attacks against honour and reputation, while the fourth relates to protection of the law against interference or attacks on privacy, home, correspondence, family, honour and reputation.

The meanings of the terms “arbitrary”, “unlawful”, “interference”, “privacy” and “correspondence” are important for understanding the full import of the limitation on the right to privacy provided in the ICCPR. To this end, the 1988 UN Human Rights Committee CCPR General Comment No. 16 on article 17 (General Comment 16), Siracusa Principles and UN resolutions and reports will be useful for unpacking the meanings of these terms as contained in the ICCPR. The General Comments elaborate on the provisions of the rights in UN treaties and should, therefore, be read together with the treaties.¹²¹ The General Comments also provide guidance in relation to policy application of the rights in UN treaties.¹²² The HRC utilises the General Comments in their decisions when determining infringement of rights. They are therefore highly persuasive documents, even though they are not legally binding on Member States.¹²³

¹²¹ American Civil Liberties Union, *Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy Under Article 17 of the International Covenant on Civil and Political Rights* (2014) <https://www.aclu.org/other/human-right-privacy-digital-age> 5 (accessed 2019-06-06) 30.

¹²² *Ibid.*

¹²³ Cusack and Pusey “CEDAW and the Right to non-discrimination and equality” 2013 14 *Melbourne Journal of International Law* 54, 58; American Civil Liberties Union “Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under

2.2.2.1 The 1988 UN Human Rights Committee CCPR General Comment No. 16 on article 17 (General Comment 16)

The General Comment 16 was prepared by the OHCHR in response to the inadequacies of the country reports on the implementation of article 17 of the ICCPR.¹²⁴ The General Comment elaborates on the provisions of the rights in the ICCPR and should therefore be read with article 17 of the ICCPR to clarify and explain the “contents and language used for the provisions”.¹²⁵

General Comment 16 highlights the UN guideline for the protection of privacy of communications as follows:

“Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.”¹²⁶

General Comment 16 interprets article 17 of the ICCPR as requiring Member States to prohibit all forms of interference with correspondence, including the interception of communications and all forms of surveillance.¹²⁷ The above quotation signifies that interference with correspondence refers to such correspondence being delivered without prior reading, tampering and/or interception. In addition, General Comment 16 outlines some of the forms of interference with communication and/or privacy and these are surveillance, interception of communications, wiretapping and recording of conversations.¹²⁸ It also prohibits the outlined interferences with privacy that is all forms of surveillance.¹²⁹

Article 17 of the International Covenant on Civil and Political Rights (2014) *A Draft report and General Comment 7*.

¹²⁴ General Comment No.16 par [2].

¹²⁵ Barbaro “Government Interference with the Right to Privacy: Is the Right to Privacy an Endangered Animal?” 2017 6 *Canadian Journal of Human Rights* 143; American Civil Liberties Union, *Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy Under Article 17 of the International Covenant on Civil and Political Rights* (2014) <https://www.aclu.org/other/human-right-privacy-digital-age> (accessed 2019-06-06) 5.

¹²⁶ General Comment par [8].

¹²⁷ *Ibid*; American Civil Liberties Union, *Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy Under Article 17 of the International Covenant on Civil and Political Rights* (2014) <https://www.aclu.org/other/human-right-privacy-digital-age> (accessed 2019-06-06) 11.

¹²⁸ *Ibid*.

¹²⁹ *Ibid*.

General Comment 16 did not, however, consider reasonable and justifiable circumstances that may warrant a State to intercept communications and/or utilise surveillance mechanisms.¹³⁰ It also did not recognise the protection of the metadata of electronic communications. This may be because technological innovation at the time did not require metadata. Metadata is nevertheless still protected under the umbrella of the right to privacy because it forms part of electronic communications.

Frank La Rue, in the report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2013 SR report) regarding the nature of metadata, stated that:

“Communications data [metadata] are storable, accessible and searchable, and their disclosure to and use by State authorities are largely unregulated. Analysis of this data can be both highly revelatory and invasive, particularly when data is combined and aggregated. As such, States are increasingly drawing on communications data to support law enforcement or national security investigations. States are also compelling the preservation and retention of communication data to enable them to conduct historical surveillance.”¹³¹

The above statement indicates that new technologies have advanced such that metadata can provide as much information about a person as the content of an electronic communication. Metadata can provide information that is as accurate as content data and its invasion and analysis by the State is equally as intrusive as the invasion into the content of an electronic communication.¹³² General Comment 16 is therefore inadequate to address current challenges to the right to privacy in the digital age as it is outdated.¹³³ A new General Comment on article 17 is needed.

¹³⁰ *Ibid.*

¹³¹ Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, A/HRC/23/40, April 17, 2013, https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf par [15].

¹³² Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 27th session, agenda items 2 and 3, A/HRC/27/37, 30 June 2014, (2014 OHCHR report) par [19]; Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12; *Digital Rights Ireland v Minister for Communications, Ireland* par [26-27,37]; Executive Office of the President, “Big Data and Privacy: A Technological Perspective (1 May 2014) <https://obamawhitehouse.archives.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy> (accessed 2021-06-10) 19.

¹³³ “[M]etadata does not include the actual content of a conversation, it nevertheless provides information (such as location, contacts and financial information) that is enough to build a comprehensive picture of any individual; Annual report of the Office of the High Commissioner for Human Rights on the Right to Privacy in the Digital age, 28th session, agenda items 2 and 3, A/HRC/28/39, 19 December 2014; Barbaro “Government Interference with the Right to Privacy: Is the Right to Privacy an Endangered Animal?” 2017 6 *Canadian Journal of Human Rights* 128; Ni “EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era” 2015 3 *Media and Communication* 54; Newell “The Massive Metadata Machine: Liberty,

Nevertheless, General Comment 16 provides a foundation to interpret the scope of the right to privacy and its permissible limitations in the ICCPR. Other UN documents, such as the Resolutions of the Human Rights Council on the right to privacy in the digital age, 2019,¹³⁴ the 2014 and 2018 reports of the OHCHR¹³⁵ and two SR reports build on the fundamental principles in General Comment 16.¹³⁶ These other documents apply the principles in General Comment 16 to the new challenges to the right to privacy thus remedying the inadequacies of the General Comment 16.

2.2.2.2 The Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR

The Siracusa Principles document assists in understanding the scope of the limitation clause in article 17. It provides definitions to frequently used terms in the ICCPR and the limitation clauses of domestic laws of Member States, Nigeria inclusive. It was prepared prior to the General Comment 16 and is the outcome of a colloquium held by the American Association for International Commission of Jurists (AAICJ) at Siracusa, Italy in 1985. The colloquium consisted of International Law experts from several countries, including Nigeria. The AAICJ stated that the abuse of the permissible limitation on human rights by Member States of the UN necessitated a detailed interpretation of the terms utilised in the ICCPR. To that end, the AAICJ

Power, and Secret Mass Surveillance in the U.S and Europe” 2014 10 *Journal of Law and Policy* 487; 2018 OHCHR report par [6].

¹³⁴ The UN General Assembly resolution on the right to privacy in the digital age, 42nd session, A/HRC/42/L.18, 24 September 2019 (2019 UN resolution on the right to privacy in the digital age); The UN General Assembly resolution on the right to privacy in the digital age, 34th session, A/HRC/RES/34/7, 23 March 2017; The UN General Assembly resolution on the right to privacy in the digital age, 28th session, A/HRC/RES/28/16, 23 March 2017; The Secretary General’s note on the right to privacy, Item 75(b), A/76/220, 23 July 2021.

¹³⁵ Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 39th session, agenda items 2 and 3, A/HRC/39/29, 3 August 2018, (2018 OHCHR report); 2014 OHCHR; The UN General Assembly resolution of the right to privacy in the digital age, 42nd session, A/HRC/42/L.18, 24 September 2019 (UN resolution on the right to privacy in the digital age).

¹³⁶ Report of the Special Rapporteur on the promotion and protection of human rights...including the right to development on Surveillance and Human Rights, A/HRC/41/35, (28 May 2019) [2019 SR report]; 2013 SR report; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/13/37 (28 December 2009) [SR report on counterterrorism] par [14-19]. These reports focus on communications surveillance. Other SR reports on the right to privacy in the digital age include the Special Rapporteur report (Joseph Cannataci), A/HRC/46/37, 25 January 2021; Special Rapporteur report, A/75/147, 27 July 2020.

organised the colloquium in order to prepare a “uniform interpretation of the limitations on rights enunciated in the Covenant”.¹³⁷

The OHCHR also referred to the Siracusa Principles when considering the limitations of the rights in the ICCPR.¹³⁸ The participants of the colloquium divided the Siracusa Principles into two parts. The first part dealt with limitation or restriction of rights in the ICCPR, while the second part dealt with derogation of rights that only occur when a state of emergency has been declared by a Member State. The limitation of rights section in the Siracusa Principles was further divided into two parts.

The first part is the general interpretive principle on the limitation of rights in the ICCPR. The second part is “the interpretive principles relating to specific limitation clauses” in the ICCPR. This relates to specific clauses such as “prescribed by law”, “in a democratic society”, “public order” and “public safety”, all of which are used in the ICCPR in relation to the limitation of rights. The Siracusa Principles document does not define the term “arbitrary”, but it defines some terms, such as necessary and proportional, which have been used to measure arbitrariness of interference with privacy.

The usefulness of the Siracusa Principles document is emphasised by the reference made to it in the 2014 OHCHR report explaining various terms contained in the ICCPR.¹³⁹ Although the Siracusa Principles document is of the same vintage as the General Comment 16 and also relates to the ICCPR, it focuses on the limitation and derogation of the ICCPR rights. Thus, the Siracusa Principles do not define other terms in the ICCPR such as privacy, correspondence and communication that are not related to limitation of rights. Nevertheless, the extensive elucidation of the clauses that are utilised in limiting the ICCPR rights makes the Siracusa Principles an important document to consider in the discussion on the permissible limitation of the ICCPR rights.

The Siracusa Principles state that restrictions of rights must be lawful, non-arbitrary, non-discriminatory and must be permitted by the treaty. Interference with privacy is permissible under article 17 of the ICCPR, within the limits of lawfulness and non-arbitrariness. The Siracusa Principles state further that every limitation of the rights in

¹³⁷ Siracusa Principles, 3.

¹³⁸ 2014 OHCHR report par [22].

¹³⁹ *Ibid.*

the ICCPR “shall be subject to the possibility of challenge to and remedy against its abusive application”.¹⁴⁰ This signifies that interference with privacy is permissible if there are adequate safeguards to prevent or challenge abuse.

The sub-sections below address the meaning of the terms “privacy”, “correspondence” and “interference” (with a focus on the requirements of “unlawfulness” and “arbitrariness”) as interpreted and/or defined in the General Comment 16, UN resolutions and reports and the Siracusa Principles.

2.2.2.3 Right to privacy in the ICCPR

Article 17 of the ICCPR provides for the protection of privacy as one of the spheres that must be shielded from unlawful or arbitrary interference. Other spheres are correspondence, family and home. General Comment 16 however expounds on the article 17 provision regarding privacy to mean the prohibition of unlawful or arbitrary intrusion on private lives of persons.¹⁴¹ This means that States through their domestic laws must determine what constitutes “private life” in their context.¹⁴²

As is shown in chapters three and four, section 14 of the Constitution of the Republic of South Africa provides for certain spheres that are considered as “private life”. Section 37 of the 1999 Nigerian Constitution does not provide for specific spheres of privacy, but the Court of Appeal in *Nwali v Ebonyi State Independent Electoral Commission* interpreted private life to include the body, life, person, thought, conscience, belief, “decisions (including his plans and choices)”, health, relationships, character, possessions and family.¹⁴³ Once privacy is defined in the context of each State, there is then an obligation upon the State to ensure that a person’s private life is protected from unlawful or arbitrary intrusion as stipulated by article 17.

2.2.2.4 Protection of correspondence and communication

General Comment 16 does not define the term “correspondence”. It does however interpret the provision on the protection of correspondence in article 17(1) of the ICCPR as follows:

¹⁴⁰ Siracusa Principles, 3 par [8].

¹⁴¹ General Comment 17 par [1]; Bilchitz “Privacy, Surveillance and the Duties of Corporations” 2016 *TSAR* 62.

¹⁴² *Ibid.*

¹⁴³ *Nwali v Ebonyi State Independent Electoral Commission* (2014) LPELR-23682 (CA) 35.

“...[T]he integrity and confidentiality of correspondence should be guaranteed *de jure* and *de facto*. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read.”¹⁴⁴

General Comment 16 indicates that the reports of the Member States on compliance with article 17 of the ICCPR to the HRC must state how interference with privacy, family, home or correspondence in practice aligns with their legislation.¹⁴⁵ State Parties of the ICCPR have an obligation to guarantee that correspondence is free from unlawful and arbitrary interference. The wording of General Comment 16 in which correspondence is required to be delivered to an addressee without being opened or read indicates that the term “correspondence” refers to written communication.¹⁴⁶ General Comment 16 recognises correspondence as distinct from communication and recognises telephonic and telegraphic communication.¹⁴⁷

The 2018 report of the Office of the High Commissioner of Human Rights (2018 OHCHR report) interprets the protection of privacy as including the protection of both the contents of a communication and the metadata.¹⁴⁸ The 2018 OHCHR report does not differentiate between correspondence and other forms of communication rather it classifies correspondence and other forms of communication carried out electronically as “a communication”.¹⁴⁹ The only distinction made in the mode of communication is whether the information gathered is the content of a communication or its metadata.¹⁵⁰ Article 17 is therefore interpreted as protecting all forms of communications and correspondence.¹⁵¹

2.2.2.5 Interference with privacy and/or correspondence

The interpretation of article 17 of the ICCPR by the General Comment that prohibits communications surveillance is one of the reasons why a new General Comment on article 17 is needed. Currently there are global threats from terrorism, cyber-attacks

¹⁴⁴ Report of the Office of the High Commissioner for Human Rights on the Right to Privacy, 32nd session, HRI/GEN/1/Rev.9 (I), General comment No.16 par [8] 8 April 1988; Ohlin “Did Russian Cyber Interference in the 2016 Election Violate International law?” 2017 95 *Texas Law Review* 1583.

¹⁴⁵ General Comment 16 par [6].

¹⁴⁶ General Comment 16 par [8].

¹⁴⁷ *Ibid.*

¹⁴⁸ Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 39th session, agenda items 2 and 3, A/HRC/39/27, 3 August 2018 (2018 OHCHR report) par [6].

¹⁴⁹ *Ibid.*

¹⁵⁰ *Ibid.*

¹⁵¹ 2018 OHCHR report par [7].

and cyber-crimes that require States to utilise communications surveillance to defend national security. The 2014 and 2018 reports of the OHCHR on the right to privacy in the digital age indicate the need for communications surveillance as a necessary tool to combat terrorism and cyber-crimes.¹⁵² However, these UN reports emphasised that communications surveillance must be regulated by laws that are non-arbitrary in terms of the ICCPR and which must be utilised for legitimate aims.

The 2014 and 2018 OHCHR reports state that the existence of a surveillance mechanism and the collection of metadata indicate interference with privacy.¹⁵³ The 2018 OHCHR report states further that the exercise of the power of a State to interfere with digital communication either through “direct tapping or penetration of digital communications infrastructure” must consider human rights.¹⁵⁴ This signifies that States retain their autonomy when controlling communications infrastructure. However, any interference that compromises the privacy of the users of such infrastructure must be subject to the permissible limitations to privacy in the ICCPR.¹⁵⁵

The 2014 and 2018 reports of the OHCHR, unlike General Comment 16, consider circumstances that may necessitate the utilisation of surveillance mechanisms, the interception of communications and the collection of metadata.¹⁵⁶ The reports therefore interpret article 17 of the ICCPR as a prohibition of unlawful and arbitrary interference with privacy and correspondence and not as a prohibition of any kind of interference with privacy and correspondence.

2.2.2.5.1 Unlawful interference with privacy and correspondence

General Comment 16 emphasises that any interference with privacy must be provided for in legislation of Member States.¹⁵⁷ It stresses that “unlawful means that no interference can take place except in cases envisaged by law”.¹⁵⁸ There must therefore be a domestic law of the Member State that permits interference with correspondence and/or privacy, otherwise such interference with privacy is

¹⁵² 2018 OHCHR report par [7]; 2014 OHCHR report par [28].

¹⁵³ *Ibid.*

¹⁵⁴ 2018 OHCHR report par [9].

¹⁵⁵ *Ibid.*

¹⁵⁶ 2018 OHCHR report par [10, 23]; 2014 OHCHR report par [28].

¹⁵⁷ General Comment 16 pars [2, 3].

¹⁵⁸ General Comment No.16 par [3]; Michael *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) 5.

unlawful.¹⁵⁹ General Comment 16 asserts that Member States must “specify in detail the precise circumstances in which such interferences may be permitted”.¹⁶⁰ However, it does not elaborate further on the consequences of a domestic law omitting to specify the circumstances of interference with privacy. Also, General Comment 16 fails to specify other provisions that must be included in a domestic law in order for the law to qualify as lawful within the definition of article 17(1) of the ICCPR.¹⁶¹

Building on General Comment 16 and in consideration of the advancement in ICT since the adoption of the ICCPR, the UN General Assembly has adopted several resolutions that assert the need for interference with privacy to be regulated by legislation.¹⁶² The UN General Assembly resolution on the right to privacy in the digital age provides broad guidelines for legislation on interference to privacy.¹⁶³ This UN resolution clearly stipulates that legislation providing for interference with privacy must be “publicly accessible, clear, precise, comprehensive and non-discriminatory”.¹⁶⁴

Articles 12(3), 18(3), 19(3), 21 and 22(2) of the ICCPR have explicit limitation

¹⁵⁹ *P.G and J.H v United Kingdom*, Application no 44787/98 pars [37,38] Judgement of the ECtHR on 25 December 2001; *Kruslin v France*, App. No. 11801/85 (1990) pars [30,32-36]; *Huvig v France* App. No. 11105/84 (1990) pars [29, 31-35]; Aquilina “Public Security Versus Privacy in Technology Law: A Balancing Act? 2010 26 *Computer Law & Security Review* 134-136; Nowak *U.N. Covenant on Civil and Political Rights: CCPR Commentary* 381.

¹⁶⁰ General Comment 16, par [8].

¹⁶¹ Deek 2015 *Virginia Journal of International Law* 348, 352.

¹⁶² The UN General Assembly resolution of the right to privacy in the digital age, 42nd session, A/HRC/42/L.18, 24 September 2019 (UN resolution on the right to privacy in the digital age); United Nations General Assembly Resolution on the Right to Privacy in the digital age, 68th session, agenda 69(b), A/RES/68/167, 21 January 2014, 2; United Nations General Assembly Resolution on the Right to Privacy in the digital age, 69th session, agenda 68 (b), A/RES/69/166,10 February 2015, 2; United Nations Human Rights Council Resolution on the Right to Privacy in the digital age, 34th session, agenda 3, A/HRC/34/L.7/Rev.1, 23 March 2017, 3; 2014 OHCHR report pars [2, 6,25].

¹⁶³ The UN General Assembly resolution of the right to privacy in the digital age, 42nd session, A/HRC/42/L.18, 24 September 2019 (UN resolution on the right to privacy in the digital age).

¹⁶⁴ The UN General Assembly resolution of the right to privacy in the digital age, 42nd session, A/HRC/42/L.18, 24 September 2019 (UN resolution on the right to privacy in the digital age); United Nations General Assembly Resolution on the Right to Privacy in the digital age,73rd session, agenda 74 (b), A/RES/73/179, 21 January 2019, 2; United Nations General Assembly Resolution on the Right to Privacy in the digital age, 71st session, agenda 68 (b), A/RES/71/199, 25 January 2017, 3; United Nations General Assembly Resolution on the Right to Privacy in the digital age, 68th session, agenda 69(b), A/RES/68/167, 21 January 2014, 2; United Nations General Assembly Resolution on the Right to Privacy in the digital age, 69th session, agenda 68 (b), A/RES/69/166,10 February 2015, 2; United Nations Human Rights Council Resolution on the Right to Privacy in the digital age, 34th session, agenda 3, A/HRC/34/L.7/Rev.1, 23 March 2017, 3; 2014 OHCHR report, pars [2, 6,25]; United Nations document “The Right to Privacy in the Digital Age”,<https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx> (accessed 5 November 2018).

clauses.¹⁶⁵ The provisions in these clauses show that a limitation of rights must be permissible by law.¹⁶⁶ Although article 17(1) of the ICCPR does not define “unlawful”, it can be defined in light of other articles of the ICCPR as a limitation for which, at the very least, provision must be made by the domestic law of a Member State.

The 2018 OHCHR report interpreted the prohibition of unlawful and arbitrary interference with privacy by pointing to the human rights principles of legality, necessity and proportionality.¹⁶⁷ Thus, the 2018 OHCHR report does not consider the terms “unlawful” and “arbitrary” as separate requirements for a permissible limitation with the right to privacy.¹⁶⁸ This signifies that the terms “unlawful” and “arbitrary” are interpreted as a joint requirement that must be considered hand-in-hand.

The 2018 OHCHR report explained that a law regulating interference with privacy can only be lawful and non-arbitrary if it is envisaged by law and not in conflict with the provisions of the ICCPR.¹⁶⁹ According to the 2018 OHCHR report, interference with privacy cannot be either unlawful or arbitrary; it can only be both unlawful and arbitrary.¹⁷⁰ It is therefore not enough for a Member State to merely enact a law that regulates interference with privacy. Domestic laws will be regarded as unlawful and arbitrary if they conflict with the provisions of the ICCPR.¹⁷¹ Nevertheless, it is important that the domestic law of Member States satisfy the requirements of legality because the necessity and proportionality principles hinge on the adequacy of the domestic law.¹⁷²

To that end, the 2018 report emphasised that:

¹⁶⁵ Article 12 of the ICCPR provides for the right to liberty of movement and the freedom to choose one’s residence; article 18 of the ICCPR provides for the right to freedom of thought, conscience and religion; article 19 of the ICCPR provides for the right to hold opinion without interference; article 21 of the ICCPR provides for the right to peaceful assembly; article 22 provides for the right to freedom of association.

¹⁶⁶ *Ibid.*

¹⁶⁷ 2018 OHCHR report par [10]; United Nations General Assembly Resolution on the Right to Privacy in the digital age, A/HRC/RES/34/7, 34th session, 23 March 2017, par [2]; Report of the UN Special Rapporteur on the right to privacy, A/HRC/40/63, 40th session, agenda item 3, 27 February 2019 par [17].

¹⁶⁸ 2018 OHCHR report par [10].

¹⁶⁹ General Comment 16 par [3].

¹⁷⁰ 2018 OHCHR report par [10].

¹⁷¹ 2014 OHCHR report par [21].

¹⁷² *Ibid.*

“States may only interfere with the right to privacy to the extent envisaged by the law and the relevant legislation must specify in detail the precise circumstances in which such interference may be permitted.”¹⁷³

The existence of a domestic law regulating interference with privacy, therefore, does not guarantee the fulfilment of the legality requirement. Nevertheless, the first stage of the requirement is that Member States must have a domestic law(s) regulating any interferences with privacy.

The Siracusa Principles define the term “prescribed by law” to mean a national law of general application that is in force at the time of the limitation of the right.¹⁷⁴ Such a law must also be clear and accessible. In addition, the domestic law must also provide for effective remedies and safeguards against abuse.¹⁷⁵ The term “lawful” in article 17 of the ICCPR should therefore be interpreted to refer to interference with privacy and correspondence that are provided for in a national law of general application that is in force at the time of the interference and which is clear, publicly accessible, precise and non-discriminatory.

2.2.2.5.2 Arbitrary interference with privacy and correspondence

General Comment 16 does not define the meaning of arbitrary interference. It expounds, however, on the inclusion of the word “arbitrary” in addition to “unlawful” in article 17(1) of the ICCPR as a means to ensure that domestic legislation of Member States conforms to the aims and objectives of the ICCPR.¹⁷⁶ Paragraphs 4 and 8 of General Comment 16 specify general guidelines to which legislation permitting interference to privacy must adhere for such interference to be non-arbitrary. These guidelines are that the domestic law providing for interference with privacy must: be reasonable; provide detailed provisions on circumstances in which interference may be permitted; provide for clear provisions on the designated authority that is to permit such interference; and the determination for permission of interference must be on a case-by-case basis.

These guidelines are reiterated by the HRC in *Hulst v Netherland* as follows:

“The Committee recalls that the relevant legislation authorizing interference with one's communications must specify in detail the precise circumstances in which such interference may be permitted and that the decision to allow such

¹⁷³ *Ibid.*

¹⁷⁴ Siracusa Principles par [B-15].

¹⁷⁵ Siracusa Principles par [A-8, B-18].

¹⁷⁶ General Comment 16 par [4].

interference can only be taken by the authority designated by law, on a case-by-case basis.”¹⁷⁷

This signifies that legislation regulating interference with correspondence and/or privacy must, at the very least, provide for the requirements stated in paragraphs 4 and 8 of General Comment 16 for such legislation to be non-arbitrary.¹⁷⁸

The 2018 report of the OHCHR states that, in addition to legality of interference with privacy, the interference must be necessary and proportional.¹⁷⁹ The 2018 report is an elaboration on the 2014 report of the OHCHR.¹⁸⁰ The 2018 report specifically states that communications surveillance may only be utilised for preventing and investigating serious crimes.¹⁸¹ General crimes are, therefore, not legitimate purposes for communications surveillance.

The 2014 report of the OHCHR states that, in addition to compliance with the ICCPR provisions, aims and objectives, limitations on interference with privacy must also be reasonable in the particular circumstances.¹⁸² It also defines “reasonableness in the circumstances” as interference on the right to privacy that is proportional and necessary.¹⁸³ Domestic laws regulating interference with privacy fulfil the reasonableness requirement when such laws are proportional and necessary. The 2014 report refers to the Siracusa Principles as a document that defines the term “arbitrary” in the ICCPR, but this is incorrect. The Siracusa Principles specifically exclude the definition of the term “arbitrary” due to time constraints.¹⁸⁴

The principle of reasonableness in international law is measured by means of three criteria. These are the means/ends or suitability test, cost effectiveness or necessity

¹⁷⁷ *Hulst v Netherland*, Communication No. U.N.Doc. CCPR/C/82/D/903/1999 (2004) par [7.7].

¹⁷⁸ *Klass v Germany* App. No. 5029/71 (1978) pars [36-55]; *Malone v United Kingdom* (1984) Series A, No.82 par [79]; In *Halford v United Kingdom*, (1997) Reports of Judgements and Decisions, 1997-III, 1004, the ECtHR stated as follows in regard to interception of communications: “[i]n the context of secret measures of surveillance or interception of communications by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights. Thus, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to circumstances in and conditions on which public authorities are empowered to resort to any such secret measures.” This statement is in line with the HRC’s requirement for legislation permitting interference with privacy.

¹⁷⁹ 2018 report par [10].

¹⁸⁰ 2018 report par [4].

¹⁸¹ 2018 report par [38].

¹⁸² Human Rights Commissioner’s Annual report on the right to privacy in the digital age, 27th session, agenda 2 &3, A/HRC/27/37, 30 June 2014, 21.

¹⁸³ *Ibid.*

¹⁸⁴ Siracusa Principles, 3.

test and cost/benefit or proportionality test.¹⁸⁵ The suitability test measures the effectiveness of the means employed with regard to the end sought.¹⁸⁶ The necessity test considers whether there are alternative means to achieve the end with minimal impairment on the right.¹⁸⁷ The proportionality test measures whether there is an “excessive or disproportionate” impact on the right.¹⁸⁸

Domestic law regulating interference with privacy fulfils the reasonableness requirement when the means employed for limitation are effective, proportional and necessary to pursue the goal of surveillance. The HRC in *Toonen v Australia* also interpreted the term “reasonableness” as implying that “any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case”.¹⁸⁹ Reasonableness, therefore, is defined as proportionality and necessity. These terms are now discussed in relation to the right to privacy.

(i) Proportionality

In explaining proportionality, the 2014 SR report on counterterrorism has recommended the traditional four-part proportionality test as the “most structured way of approaching the inquiry into whether a limitation on the right to privacy is arbitrary”.¹⁹⁰ The test requires that there be a legitimate aim for the limitation of the right to privacy.¹⁹¹ Also, the legitimate aim must be rationally connected to the measure taken to limit the right.¹⁹² In addition, the impairment on the right to privacy must be minimal.¹⁹³ Finally, a fair balance struck between the legitimate aim pursued and the right to privacy.¹⁹⁴

¹⁸⁵ Ortino “From ‘non-discrimination’ to ‘reasonableness’: A Paradigm Shift in International Economic Law?” (April 2005) *Jean Monnet Working Paper 01/05 New York University School of Law* 34; Trachtman “Trade and ... Problems, Cost-Benefit Analysis and Subsidiarity” 1998 9 *European Journal of International Law* 33; Grainne de Búrca “The Principle of Proportionality and its Application in the EC Law” 1994 13 *The Yearbook of European Law (YEL)* 113; Jan “Proportionality Revisited” 2000 27 *Legal Issues of Economic Integration* 241.

¹⁸⁶ Ortino “From ‘non-discrimination’ to ‘reasonableness’” *Jean Monnet Working Paper* 34.

¹⁸⁷ *Ibid.*

¹⁸⁸ Ortino “From ‘non-discrimination’ to ‘reasonableness’” *Jean Monnet Working Paper* 35.

¹⁸⁹ Communication No. U.N.Doc. CCPR/C/50/D/488/1992 (1994) par [8.3].

¹⁹⁰ SR report on counterterrorism; 2013 SR report [28-29]; Novak *U.N. Covenant on Civil and Political Rights: CCPR Commentary* 2ed (2005), 378.

¹⁹¹ American Civil Liberties Union, *Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy Under Article 17 of the International Covenant on Civil and Political Rights* (2014) <https://www.aclu.org/other/human-right-privacy-digital-age> (accessed 2019-06-06) 24.

¹⁹² *Ibid.*

¹⁹³ *Ibid.*

¹⁹⁴ *Ibid.*

(ii) Necessary

The OHCHR reports define proportionality, but do not define the term “necessary”. The Siracusa Principles however, define the term “necessary” as a limitation that:

- “ (a) is based on one of the grounds justifying limitations recognized by the relevant article of the Covenant;
- (b) responds to a pressing public or social need;
- (c) pursues a legitimate aim; and
- (d) is proportionate to that aim.”

This definition creates further requirements to which statutory regulations permitting interference with privacy must adhere. The “necessity” requirement focuses on the aim that the limitation pursues. The Siracusa Principles stipulate the aims for limitation that international law will consider reasonable. They also highlight that the aim pursued must be legitimate, a pressing public or social need and aligned with recognised aims for limitation of right in the ICCPR. The “necessity” requirement ensures that the legitimate aim pursued is as provided in international law.

The discussion will now move to other treaties protecting the right to privacy.

2.2.3 The United Nations Convention on the Rights of the Child

The UN Convention on the Rights of the Child (CRC) is a treaty that aims to promote the basic needs of children as fundamental human rights.¹⁹⁵ The CRC is focused on eliminating the discrimination of a child, ensuring the child’s best interests and the right to survival and development, as well as respecting the child's views.¹⁹⁶ One may ask why there is a need for a separate treaty for children since the ICCPR applies to everyone. The answer is that the CRC is needed to provide specific protection for children because they are dependent on adults for physical and psychological care and are defined as vulnerable persons in society.¹⁹⁷

Also, the rights of children are subject to their parents or guardians, who ordinarily should foster the interests of the child. However, this is not always the case. It is thus important to define specifically the rights of the child in international treaties in order to guide domestic legislation of Member States on certain standards of care for a

¹⁹⁵ Jupp “The United Nations Convention on the Rights of the Child: An Opportunity for Advocates” 1990 12 *Human Rights Quarterly* 130.

¹⁹⁶ Johnson “Strengthening the Monitoring of and Compliance with the Rights of the African Child” 2015 23 *International Journal of Children's Rights* 370.

¹⁹⁷ Macenaite “From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation” 2017 19 *New Media & Society* 767.

child.¹⁹⁸ This signifies that the domestic legislation of Member States on the rights of a child must reflect the principles in the CRC. With regard to the right to privacy of the child, article 16 of the CRC provides as follows:

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

The wording of the CRC overlaps with that of the ICCPR, but the former applies to children only. The application of the wording of article 17 of the ICCPR should apply to article 16 of the CRC because of the similarity of the provisions. Therefore, the definitions of lawful and arbitrary in section 2.1.2.3 above also apply to article 16 of the CRC.

One of the aims of the inclusion of the right to privacy in the CRC is to protect children from undue publicity and labelling.¹⁹⁹ In recent times, there has been an increase in the scholarship on the protection of the right to privacy of children because of the increased exposure of children on social media platforms.²⁰⁰ Also, increased internet usage exposes children to more risks on social platforms.²⁰¹

In this study, the discussion on the rights to privacy of the child will only be approached in relation to communications surveillance. Even then, the same standard of lawfulness and non-arbitrariness applies to a child’s communications as to that of adults. Furthermore, article 17 of the ICCPR includes children in its general provision on the right to privacy, family, home and correspondence. This is because the wording

¹⁹⁸ Ruck, Keating, Saewyc, Earls and Ben-Arieh “The United Nations Convention on the Rights of the Child: Its Relevance for Adolescents” 2015 26 *Journal of Research on Adolescence* 16.

¹⁹⁹ UN Committee on the Rights of the Child, General Comment No. 10 on the CRC, 18 par [64], 2007; Niamh “An Analysis of the Extent of the Juvenile Offender’s Right to Privacy: Is the Child’s Right to Privacy Circumvented by Public Interest?” 2011 19 *European Journal of Crime, Criminal Law and Criminal Justice* 120.

²⁰⁰ Sorensen “Protecting Children’s Right to Privacy in the Digital Age: Parents as Trustees of Children’s Rights” 2016 26 *Children’s Legal Rights Journal* 158; Dell’Antonia “Don’t Post About Me on Social Media, Children Say” *The New York Times* (March 8, 2016), <https://archive.nytimes.com/well.blogs.nytimes.com/2016/03/08/dont-post-about-me-on-social-media-children-say/> (accessed 2019-03-10).

²⁰¹ Livingstone and Helsper “Gradiation in Digital Inclusion: Children, Young People and the Digital Divide” 2007 9 *New Media & Society* 671; Livingstone, Carr and Byrne “One in Three: Governance and Children’s Rights” *Global Commission on Internet Governance Paper Series No.22* 5; Bartel “Parents’ Growing Pains on Social Media: Modeling Authenticity” 2015 *Character and Social Media* 51, 63; Shmueli and Blecher-Prigat “Privacy for Children” 2011 42 *Columbia Human Rights Law Review* 759; Steinberg “Sharenting: Children’s Privacy in the Age of Social Media” 2017 66 *University of Florida Law Scholarship Repository* 839.

of article 17 of the ICCPR in which “no one” shall be subjected to unlawful or arbitrary interference to privacy is to the effect that all persons, children and adults included, are entitled to their right to privacy.

2.2.4 The International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families

The International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW) is a UN treaty which seeks to protect migrants’ rights.²⁰² The ICRMW aims to balance the human rights of migrant workers with the rights of States to control their borders.²⁰³ Article 2 of the ICRMW defines a migrant worker as

“a person who is to be engaged, is engaged or has been engaged in a remunerated activity in a State of which he or she is not a national”.

This signifies that the ICRMW is only applicable to migrants in paid, self and/or other employment in a State other than own.²⁰⁴ **The ICRMW is also applicable to family members of migrant workers, but does not apply to all categories of migrants, for example refugees and students.**²⁰⁵ This does not mean that other categories of migrants not covered by the ICRMW are exempt from human rights protection.²⁰⁶ It only signifies that other treaties, such as the ICCPR, apply to those categories of migrants.

Article 14 of the ICRMW protects the right to privacy of all migrant workers and their families and provides as follows:

“No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and members of his or her family shall have the right to the protection of the law against such interference or attacks.”

²⁰² Dembour and Kelly (eds) *Are Human Rights for Migrants?* (2011) 32.

²⁰³ Alan “The Triangle that could Square the Circle? The UN International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, the EU and the Universal Periodic Review” 2015 17 *European Journal of Migration and Law* 44; Fudge “Precarious Migrant Status and Precarious Employment: The Paradox of International Rights for Migrant Workers” 2012 34 *Comparative Labour Law & Policy Journal* 103.

²⁰⁴ Article 2(2) of the ICRMW.

²⁰⁵ Article 3 of the ICRMW.

²⁰⁶ Ruhs “The Human Rights of Migrant Workers: Why Do So Few Countries Care? 2012 56 *American Behavioral Scientist* 1280.

The ICRMW protects the migrant worker's privacy, family, correspondence and communications against unlawful interference. The ICRMW, unlike the UDHR, the ICCPR and the CRC, protects communications as a separate component from correspondence. The distinction between correspondence and communications places an emphasis on the protection of the migrant workers' communications against unlawful and/or arbitrary interference. Otherwise, the provisions of the ICRMW and the ICCPR are similar and, like the CRC, the definitions of "privacy", "correspondence", "communication", "interference", "unlawful" and "arbitrary" in the ICCPR apply to the ICRMW. The human rights in the ICRMW and the CRC are an expansion of the rights in the UDHR, ICCPR and International Covenant on Economic, Social and Cultural Rights, 1966 (ICESCR) that are then applied to specific groups of persons such as children and migrants.²⁰⁷

2.2.5 The need for a new General Comment on article 17

The terms "privacy", "correspondence" and "communications", "unlawfulness" and "arbitrariness" have been discussed with reference to the General Comment 16, UN resolutions, reports and the decisions of the HRC. These documents do not have any binding authority on Member States. Although they clarify the terms in the ICCPR, they are still open to various interpretations by Member States.²⁰⁸ Therefore, the documents do not provide conclusive and authoritative guidance on the statutory regulation of communications surveillance.²⁰⁹ Furthermore, the HRC has not adjudicated sufficient cases on communications surveillance to develop definite standards that can provide authoritative guidance for the statutory regulation of communications surveillance. In addition, the guidelines provided by the HRC in its 2018 OHCHR report have been extrapolated from the ECtHR and have not been tested by the HRC.²¹⁰

As shown above, General Comment 16, being a 1988 document, is outdated and is not aligned with the demands on the right to privacy in the digital age. A new General

²⁰⁷ Alan "The Triangle That Could Square the Circle? The UN International Convention on the Protection of Migrant Workers and Members of Their Families, the EU and the Universal Periodic Review" 2015 17 *European Journal of Migration and Law* 45; ICESCR, 16 December 1966, GA. Res 2200A (XXI) (entered into force 3 January 1976).

²⁰⁸ Deeks 2015 *Virginia Journal of International Law* 306.

²⁰⁹ Georgieva 2015 *Utrecht Journal of International and European Law* 116-117; Sinha 2013 *Loyola Law Review*, 945.

²¹⁰ 2018 OHCHR Report pars [36-38].

Comment will unify the UN's interpretation of article 17 of the ICCPR, which is scattered over various resolutions and reports, as well as clarifying the interpretational difficulties of the terms utilised in article 17.²¹¹

Ultimately, the principles of international law with regard to interference with privacy, correspondence and communications are that:

- Interference with privacy must be prescribed by the domestic law of a Member State. Such domestic law must be of general application, clear and accessible; and
- Interference with privacy, correspondence and communications must be reasonable.

International law has been able to provide a general guideline for the regulation of interference with privacy that is lawful and non-arbitrary. However, the interpretation provided by various resolutions, reports and General Comment 16 has not been able to describe authoritatively the minimum requirements that a law regulating communications surveillance must possess in order to be lawful and non-arbitrary.²¹² As shown in section 2.5 below, countries that are signatories to the ECHR and/or the EU Charter on Fundamental Rights (the EU Charter) also faced the same dilemma until the ECtHR developed minimum requirements for the regulation of communications surveillance. Nigeria can glean some very valuable lessons from the ECtHR's minimum requirements.

The next section on African regional law demonstrates the lack of guidance by the African regional law on the regulation of communications surveillance. This reiterates the need to draw more concrete lessons from European regional law.

2.3 African regional laws on the regulation of communications surveillance

In setting out the regional law regulating communications surveillance, this section discusses the general provisions of the African Union (AU) on the right to privacy. It also analyses the guidelines on the regulation of communications surveillance

²¹¹ American Civil Liberties Union, *Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy Under Article 17 of the International Covenant on Civil and Political Rights* (2014) <https://www.aclu.org/other/human-right-privacy-digital-age> (accessed 2019-06-06) 28.

²¹² Cannataci, "Working Draft Legal Instrument on Government-Led Surveillance and Privacy" (28 February 2018) https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf (accessed on 2019-10-21) 2.

provided in the Declaration on Freedom of Expression and Access to Information (the 2019 Declaration).²¹³ The African Charter on Human and Peoples' Rights, 1981(ACHPR) does not provide for the right to privacy. Subsequent treaties such as the African Charter on the Rights and Welfare of the Child, 1990 (ACRWC) and the African Union Convention on Cyber Security and Personal Data Protection, 2014 (AUCCP), protect the right to privacy of children and personal data respectively.²¹⁴ Hence there is no explicit protection of the right to privacy that applies to everyone in African regional law. Despite the absence of the protection of the right to privacy in the ACHPR, it is necessary to have a sense of its provisions on the permissible limitations of other human rights. This will help align any recommendations gathered from the European regional laws to the African context.

2.3.1 The African Charter on Human and People's Rights

The ACHPR is an African regional treaty that aims to protect the fundamental human rights of persons within the African territory. It, however, fails to provide for the right to privacy. As shown below, this does not mean that privacy is not protected in the African context.

The ACHPR is subject to the rules of international human rights law in implementing its provisions in the African region.²¹⁵ Article 30 of the ACHPR establishes the African Commission of the Human and Peoples' Rights (AU Commission). The Protocol to the ACHPR (the ACHPR Protocol) establishes the African Court on Human and Peoples' Rights (ACtHPR).²¹⁶ The ACHPR Protocol extends the jurisdiction of the ACtHPR to all cases and disputes concerning the interpretation and application of the ACHPR,

²¹³ The African Union is an African continental organisation launched on July 2002 having being preceded by the Organisation of African Unity (OAU, 1963-1999). The AU consists of 55 Member States including Nigeria and South Africa.

²¹⁴ African Charter on Human and Peoples' Rights, adopted on 27 June 1981 at Nairobi, Kenya and entered into force on 21 October 1986, OAU Doc, CAB/LEG/67/3 Rev. 5, 21 ILM 58 (1982).

²¹⁵ The ACHPR was adopted by the Organisation of African Unity (now African Union) on the 1 June 1981. It entered into force on the 21 October 1986, 21 I.L.M 58; *Constitutional Rights Project & Another v Nigeria* (2000) African Human Rights Law Report (AHRLR) 191 par [48]; Decision of the African Commission on Human and Peoples' Rights, 31st October 1998; Enabulele "Incompatibility of National Law with the African Charter on Human and Peoples' Rights: Does the African Court on Human and Peoples' Rights Have the Final Say" 2016 16 *AHRLR* 22.

²¹⁶ ACHPR Protocol, June 10, 1998, entered into force on June 25, 2004. The Court started operations in 2006; *African Court in Brief* African Court on Human and Peoples' Rights, <http://www.african-court.org/en/index.php/2-uncategorised/47-african-court-in-brief> (accessed 2019-06-12); Nigeria ratified the ACHPR Protocol on the 20th May 2004.

the ACHPR Protocol and any human rights instrument ratified by Member States of the African Union (AU).²¹⁷ Article 3 of the ACHPR Protocol provides as follows:

- “1. The jurisdiction of the Court shall extend to all cases and disputes submitted to it concerning the interpretation and application of the Charter, this Protocol and any other relevant human rights instrument ratified by the States concerned.
2. In the event of a dispute as to whether the Court has jurisdiction, the Court shall decide.”

The significance of article 3 is that the jurisdiction of the Court is not limited to the treaties of the AU alone. It extends to other human rights treaties including international treaties, that the disputing parties have ratified.²¹⁸ However, the disputing parties must submit their complaint to the AU Commission before approaching the ACtHPR. Also, the ACtHPR cannot accept cases from States that have not ratified the ACHPR Protocol. Nigeria has ratified the ACHPR Protocol and so the ICCPR can be considered if there is an allegation of infringement on the right to privacy.²¹⁹

Articles 60 and 61 of the ACHPR empower the AU Commission to draw inspiration from the international law on human rights, particularly UN treaties and declarations on human rights. This signifies that the AU Commission can draw inspiration from the ICCPR, the CRC and the UDHR. As a result, where the ACHPR does not provide for certain human rights that are recognised by other international human rights treaties, such as the right to privacy, the AU Commission and the ACtHPR can adjudicate on such rights in compliance with articles 60 and 61 of the ACHPR.²²⁰

²¹⁷ Article 3 of the ACHPR Protocol; *Malengo v Tanzania* No. 030/2015, Judgment, ACtHPR 18, (July 4, 2019).

²¹⁸ In the Consolidated Matter of *Tanganyika Law Society and the Legal and Human Rights Centre v Tanzania* and *Mtikila v Tanzania*, No. 009/2011 & 011/2011, Judgment, ACHPR (June 14, 2013) pars [122-123]; Yakaré-Oulé, Reventlow and Curling “The Unique Jurisdiction of the African Court on Human and Peoples’ Rights: Protection of Human Rights beyond the African Charter” 2019 33 *Emory International Law Review* 204, 207.

²¹⁹ Nigeria ratified the Protocol to the ACHPR on 20 May 2004 [https://au.int/sites/default/files/treaties/36393-sl-PROTOCOL_TO_THE_AFRICAN_CHARTER_ON_HUMAN_AND_PEOPLESRIGHTS_ON_T HE_ESTABLISHMENT_OF_AN_AFRICAN_COURT_ON_HUMAN_AND_PEOPLES_RIGHTS. pdf](https://au.int/sites/default/files/treaties/36393-sl-PROTOCOL_TO_THE_AFRICAN_CHARTER_ON_HUMAN_AND_PEOPLESRIGHTS_ON_THE_ESTABLISHMENT_OF_AN_AFRICAN_COURT_ON_HUMAN_AND_PEOPLES_RIGHTS.pdf) (accessed on 2018-12-28).

²²⁰ Article 27(2) of the ACHPR. Although, the ACHPR does not provide for a right to privacy, individuals can still seek redress from the ACtHPR for infringements on their privacy in their personal capacity. The *locus standi* of individuals to present cases of infringement to the ACtHPR is subject to article 34(6) of the ACHPR Protocol. Article 34(6) of the ACHPR Protocol provides that the applicant’s State must have signed a declaration that the ACtHPR can assume jurisdiction on applications by individuals and non-governmental organisations (NGOs). Nigeria and South Africa have not signed this special declaration. *Media Rights Agenda v Nigeria* 224/98 (6th November 2000) par [51]. In the *Media Rights* case, the ACHPR did not provide for a right to public trial hence the ACtHPR relied on General Comment 13 of the HRC on the right

The provisions of the ACHPR on human rights are only limited by “the rights of others, collective security, morality and common interest”.²²¹ Since the ACHPR does not make provision for the right to privacy, the interpretation of the right by the ACtHR would have to take place by way of reliance on international treaties. It follows therefore that, the limitation of the right to privacy can also be inferred from international treaties.²²²

The ACtHPR has not dealt with cases where it has had to consider the violation of privacy rights. Nonetheless, the ACtHPR has shown its willingness to align its decisions in favour of an applicant whose claim is provided for in another human rights treaty to which their State is a party to or even in customary international law. For example, in *Anudo v Tanzania*, the ACtHPR delivered a judgement in favour of the applicant based on customary international law in respect of the violation of his right to nationality.²²³ The ACtHPR resorted to customary international law because neither the ACHPR, the ICCPR or other treaties ratified by Tanzania provided for a right to nationality.

Article 27(2) of the ACHPR provides for the limitation of rights in the ACHPR. Since the right to privacy is not one of the rights recognised in the ACHPR, article 27(2) of the ACHPR does not apply. The ICCPR will therefore be applicable to any dispute against Nigeria before the ACtHR regarding the interference with the right to privacy.

2.3.2 The African Charter on the Rights and Welfare of the child

The African Charter on the Rights and Welfare of the Child, 1990 (ACRWC), recognises the right to privacy as a human right to be protected by legislation.²²⁴ The ACRWC was adopted after the ACHPR and the ACHPR Protocol. Article 10 of ACRWC provides that:

“no child shall be subject to arbitrary or unlawful interference with his privacy, family[,] home or correspondence, or the attacks upon his honour or reputation,

to a fair trial for its decision; Abdi “Derogation from Constitutional Rights and Its Implication under the African Charter on Human and People's Rights” 2013 17 *Law Democracy & Development* 92.

²²¹ Article 27(2) of the ACHPR.

²²² The ACtHPR has in several cases based its decisions on, in addition to ACHPR, international and sub-regional treaties like ICCPR and the ECOWAS treaty No. 001/2014, Judgment, ACtHPR, (November 18, 2016); *Konaté v Burkina Faso*, App. No. 004/2013, Judgment, ACtHPR, 176(8) (December 5, 2014); *Abubakari v Tanzania* No. 007/2013, Judgment, ACtHPR, (June 3, 2016); *African Commission on Human and Peoples Rights v Libya* No. 002/2013, Decision, African Commission on Human and Peoples Rights, 97 (June 3, 2016).

²²³ No. 012/2015, Judgment, ACtHPR, 88 (22 March 2018); *Chacha v Tanzania* No. 003/2012, Ruling on Admissibility, ACHPR 157 (March 28, 2014).

²²⁴ Nigeria ratified the ACRWC on 23 July 2001.

provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the rights to the protection of the law against such interference.”

This provision also prohibits unlawful and arbitrary interference to privacy and correspondence. There is no equivalent provision in the ACHPR. There is also no definitional guidance for the phrase “unlawful and arbitrary interference” in the ACHPR. It follows therefore that the use of the words “unlawful” and “arbitrary” in article 10 of the ACRWC were derived from international conventions such as the ICCPR and the CRC, and the same definition that applies to them should also apply to the ACRWC. Therefore, interference with privacy, family, home and correspondence of a child in a State has ratified the ACRWC must be regulated by way of a law of general application that is clear and accessible. Also, interference with privacy, home, family and correspondence of a child subject to the ACRWC must be reasonable and proportional.

2.3.3 The African Union Convention on Cyber Security and Personal Data

The focus of the African Union Convention on Cyber Security and Personal Data Protection, 2014 (AUCCP) is to provide guidelines to its Member States on the regulation of electronic commerce, the protection of personal information and the strengthening of cyber-security.²²⁵ The AUCCP aims to provide minimum standards to its Member States on the processing of personal data and also to provide a harmonised regulatory framework on cyber-security.²²⁶ In a bid to promote cyber security and combat cybercrime, the AUCCP recommends the classification of certain activities as cybercrimes.²²⁷ These classifications aid the trans-boundary punishment of cybercriminals in the event of a request for extradition.²²⁸ The classification of cybercrimes also assists in clarifying the activities that amount to cybercrime for the purpose of fulfilling the double criminality principle in extradition law.²²⁹

²²⁵ Article 1 of the AUCCP refers to Personal information as personal data in the AUCCP; Report of the Experts Session of the Extraordinary Conference of African Union Ministers in Charge of Communication and Information Technologies (CITMC) http://registry.africa/wp-content/uploads/2017/06/CITMC_ExpertsReport_ORTambo.pdf (accessed on 2018-10-17); Orji, “The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability” 2018 12 *Masaryk University Journal of Law & Technology* 92.

²²⁶ Orji “The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability” 2018 12 *Masaryk University Journal of Law & Technology* 113.

²²⁷ Article 29 of the AUCCP.

²²⁸ Gardocki “Double Criminality in Extradition Law” 1993 27 *Israel Law Review* 289-300.

²²⁹ Williams “The Double Criminality Rule and Extradition: A Comparative Analysis” 1991 15 *Nova Law Review* 581. Double criminality principle in extradition law states that the act or omission for

The protection of cybersecurity is important as the internet operates across national borders, as do cybercrimes. A survey of internet users in Africa between 2000 and 2019 indicates a growth from about 4.5 million to 525 million.²³⁰ The proliferation of the internet in Africa has activated a shift in the economic, social and political climate on the Continent. This increase in internet usage in Africa has led to a rise in electronic commerce and a massive processing of personal information, hence the need to protect personal information of individuals, prevent cybercrimes and ensure cybersecurity. It is the duty of a State to prevent trans-boundary harm, like cybercrime and as a result the AUCCP was tabled for ratification by the AU.²³¹

Unfortunately, several countries, including Nigeria and South Africa, have not ratified the AUCCP.²³² The refusal to ratify this treaty may be as a result of the criticism of the AUCCP which includes lumping cybersecurity and cybercrimes together.²³³ This is seen as a disregard of the international guidelines for a human rights approach to legislating cybersecurity.²³⁴ The AUCCP has also been criticised for criminalising hate speech and xenophobic activities, thus disregarding “firmly established principles” of international law on the right to freedom of expression.²³⁵ This means that the vision of a harmonised regulatory framework on cybersecurity is unlikely.²³⁶

Nevertheless, Nigeria has enacted legislation that prohibits cybercrimes and that categorises certain activities, including the unlawful interception of communications, as cybercrimes.²³⁷ The Cybercrimes (Prohibition, Prevention, etc) Act, 2015 (CPPA) is one of the statutes regulating communications surveillance in Nigeria. Unfortunately,

which the person under extradition order is to be prosecuted must be recognised as an offence in the State that he is to be extradited from and the State requesting the extradition.

²³⁰ Miniwatts Marketing Group, Internet World Stats “Internet Usage Statistics for Africa” (June 30, 2019) <http://www.internetworldstats.com/stats1.htm> (accessed 2019-07-28).

²³¹ African Union, Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report, Addis Ababa Ethiopia: African Union (2008) https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/2_Draft_Report_Study_on_Telecom_ICT_Policy_31_Mar_ch_08.pdf (accessed 2019-2-11).

²³² Centre for Human Rights, University of Pretoria, “The Right to Privacy in the Digital Age: Privacy and Cybersecurity” (June 2021) *Massive Open Online Course (MOOC)* 12.

²³³ *Ibid.*

²³⁴ Centre for Human Rights, University of Pretoria, “The Right to Privacy in the Digital Age: Privacy and Cybersecurity” (June 2021) *Massive Open Online Course (MOOC)* 12.

²³⁵ Centre for Human Rights, University of Pretoria, “The Right to Privacy in the Digital Age: Privacy and Cybersecurity” (June 2021) *Massive Open Online Course (MOOC)* 12.

²³⁶ Centre for Human Rights, University of Pretoria, “The Right to Privacy in the Digital Age: Privacy and Cybersecurity” (June 2021) *Massive Open Online Course (MOOC)* session 4, 12.

²³⁷ Cybercrimes (Prohibition, Prevention, Etc) Act, 2015.

the provisions of the CPPA on the regulation of communications surveillance are not in compliance with international law, thus the need for reform and this thesis. The defects in the Nigerian law are discussed in detail in chapters four and five.

South Africa has also not ratified the AUCCP but has a newly enacted statute, the Cybercrimes Act, 2020 that categorises communications surveillance as a cybercrime.²³⁸ The Electronic Communications and Transactions Act (ECTA) also criminalises cybercrimes and the unlawful interception of communications.²³⁹ The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) is the primary law on the regulation of communications surveillance and creates offences for the unlawful interception of communications.²⁴⁰ The RICA, which is discussed in chapter 3 is a more developed statute than the laws regulating communications surveillance in Nigeria. The principles gathered from this chapter will, therefore, assist in explaining why RICA is a better statute than Nigeria's statutes on interception of communications. Chapter 3 will also assist in providing guidance on the lessons that Nigeria can learn from the RICA and the loopholes which she is to avoid.

The refusal of South Africa and Nigeria's reluctance to ratify the AUCCP signifies disagreement with its provisions, as opposed to the criminalisation of cybercrimes. This is clear by virtue of Nigeria and South Africa's enactment of domestic laws prohibiting cybercrimes. The AUCCP does not provide any guidelines for regulating communications surveillance but does provide for the processing of personal data. The AUCCP defines personal data as:

“any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.”

The definition of personal data in the AUCCP signifies that the contents of electronic communications and its metadata qualifies as personal data. Communications surveillance involves the processing of both the contents and metadata of electronic

²³⁸ S.3 of the Cybercrimes Act 19 of 2020; S.86 of the Electronic Communications and Transactions Act 25 of 2002.

²³⁹ S.86 of the Electronic Communications and Transactions Act 25 of 2002.

²⁴⁰ S.2 of the Regulation of the Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

communications. The provisions of the AUCCP are therefore applicable to the activities of the State in communications surveillance.

Article 9(1)(d) of the AUCCP provides that the processing of personal information for the purpose of public security, defence, research, State security and criminal prosecution is excluded from its purview.²⁴¹ Article 10(5) of the AUCCP provides that a legislative or regulatory act of a Member State must provide for the processing of personal data by the State, its agencies or a third-party processing data on the State's behalf for certain activities. The activities in the processing of personal data that require statutory regulation are matters relating to state security, crime prevention, population surveys or any personal data revealing sensitive information including race, political affiliation and ethnicity.²⁴² Consequently, the processing of personal information by the State for the purposes set out in article 10(5) of the AUCCP must be prescribed by law. The AUCCP does not provide further guidelines for such statutory or regulatory act. The only guideline provided by the AUCCP that is useful for laws regulating communications surveillance within the African region is that processing of personal data by the State for certain specified purpose must be provided by law.

2.3.4 The Declaration on Freedom of Expression and Access to Information

2.3.4.1 The protection of the right to privacy in the 2019 Declaration

The 2019 Declaration was adopted by virtue of article 45 of the ACHPR.²⁴³ Member States have to assimilate the 2019 Declaration in their domestic laws. It is, however, a soft-law instrument and not binding on Member States, but it may have a persuasive effect on domestic courts and the ACtHR. Principle 40(1) of the 2019 Declaration recognises the right to privacy as a human right in Africa as it provides that everyone has a right to privacy and this includes “the confidentiality of their communications and the protection of their personal information”. The 2019 Declaration also grants individuals the right to communicate anonymously over communications networks and

²⁴¹ S.6 of the Protection of Personal Information Act of 4 of 2013 (POPIA) deviates from the AUCCP as it exempts the processing of personal information for national security and some other activities from its regulation. The effect of this exemption is discussed in chapter three.

²⁴² Article 10(5) AUCCP.

²⁴³ Adopted by the African Commission on Human and People's Rights, 65th ordinary session, 21 October to 10 November 2019, Banjul, Gambia; Article 9 of the ACHPR.

encrypt their communications.²⁴⁴ Member States are prohibited from formulating or implementing laws that will compel communications service providers (CSPs) to disable or weaken encryptions unless for justifiable purposes that align with international human rights law.²⁴⁵

Principle 40(3) of the 2019 Declaration prohibits Member States from mass surveillance (bulk surveillance). It further provides that targeted surveillance is permissible only when it is:

“authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.”²⁴⁶

Principle 40(3) signifies that domestic law on communications surveillance must comply with international law. This connotes that a Member State, like Nigeria, that is yet to domesticate the ICCPR, must also adhere to international law standards when regulating communications surveillance.

Principle 41(3) of the 2019 Declaration provides guidelines for domestic law of Member States in regulating communications surveillance as follows:

“provide adequate safeguards for the right to privacy, including:

- a. the prior authorisation of an independent and impartial judicial authority;
- b. due process safeguards;
- c. specific limitation on the time, manner, place and scope of the surveillance;
- d. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
- e. proactive transparency on the nature and scope of its use; and
- f. effective monitoring and regular review by an independent oversight mechanism.”²⁴⁷

Principle 41(3) uses the word “includes” to signify that the list for adequate safeguards for the right to privacy is not exhaustive. These guidelines are broad like those provided in international law. The 2019 Declaration is the only law that provides guidelines for communications surveillance in the African regional law and will be utilised to recommend reforms for Nigeria in chapter five.

²⁴⁴ Principle 40(3) of the 2019 Declaration.

²⁴⁵ *Ibid.*

²⁴⁶ Principle 41(2) of the 2019 Declaration.

²⁴⁷ Principle 41(3) of the 2019 Declaration.

2.3.4.2 Limitation of right to privacy in the 2019 Declaration

Principle 9(1) of the 2019 Declaration provides that limitations on the rights to freedom of expression and access to information is justifiable if it:

- “ (a) is prescribed by law;
- (b) serves a legitimate purpose; and
- (c) is a necessary and proportionate means to achieve the state aim in a democratic society.”

Principle 9(2) of the 2019 Declaration clarifies the meanings on the precise meaning of the terms used in Principle 9(1). Principle 9(2)(a) states that “prescribed by law” refers to the law being “clear, precise, accessible and foreseeable”. The law must also be “overseen” by an independent body that is “not arbitrary or discriminatory”.²⁴⁸ Principle 9(2)(c) states that a domestic law that is regarded as “prescribed by law” must also provide for an effective safeguard against abuse and this includes an avenue for appeal to “independent and impartial courts.”²⁴⁹ Member States may provide additional avenues that can effectively safeguard rights against abuse. These definitions of “prescribed by law” are similar to those in international law discussed in 2.2. above.

Principle 9(3) of the 2019 Declaration provides for the legitimate aims for the limitation of the freedom of expression. These are to: “preserve respect for the rights or reputation of others; protect national security, public order or public health”. Domestic law of Member States must ensure that freedom of expression is not restricted for aims that are different from those prescribed in the 2019 Declaration.

Lastly, Principle 9(4) provides that the limitation of the rights to freedom of expression and access to information is regarded as “necessary” and “proportionate” when:

- “ a. it originate from a pressing and substantial need that is relevant and sufficient;
- b. have a direct and immediate connection to the expression and disclosure of information, and be the least restrictive means of achieving the stated aim; and
- c. be such that the benefit of protecting the stated interest outweighs the harm to the expression and disclosure of information, including with respect to the sanctions authorised.”

²⁴⁸ Principle 9(2)(b) of the 2019 Declaration.

²⁴⁹ Principle 2(c) of the 2019 Declaration.

The factors for determining “necessary” and “proportionate” in Principle 9(4)(a)-(c) are a conflation of international law’s four-part proportionality test and the Siracusa Principles’ interpretation of “necessary”.²⁵⁰ It can be deduced that the compilation of these factors are influenced by international law’s general principles for limitation of rights. The factors can therefore be applied to extend to other rights, the right to privacy inclusive.

As discussed briefly in chapter one, section 45 of the 1999 Nigerian Constitution limits both the rights to privacy (section 37) and right to the freedom of expression (section 39) among other rights.²⁵¹ Since the same limitation applies to both rights, the requirements for limiting the right to freedom of expression in the 2019 Declaration extends to the right to privacy.²⁵² Hence, Nigerian courts must interpret the limitation clause for the right to privacy in section 45(1) of the 1999 Nigerian Constitution to reflect the factors in Principle 9(4) of the 2019 Declaration. This is because the ACHPR has been domesticated and has a more persuasive effect on Nigerian courts than the ICCPR.²⁵³ The 2019 Declaration will therefore be one of the laws used in recommending the correct way to interpret section 45(1) of the 1999 Nigerian Constitution in chapter five.

2.3.5 The jurisdiction of the ACtHR in respect of right to privacy adjudication

The ACtHR can adjudicate cases dealing with the right to privacy where a State has ratified a treaty and/or has enacted domestic law that recognises the right.²⁵⁴ Also, the ACtHR will apply limitations to the right to privacy according to the treaty in issue. Therefore, the ACtHR can adjudicate on cases relating to interference with privacy, correspondence and communication and by extension matters pertaining to communications surveillance.

²⁵⁰ This is discussed in sections 2.2.3(ii)(a) & b above.

²⁵¹ These other rights are: the freedom of thought, conscience and religion; freedom of assembly and association; freedom of movement. Access to information is not a right under the Nigerian Bill of Rights however the Freedom of Information Act, 2011. empowers people to access information. This is discussed in chapter four of the thesis.

²⁵² Principle 9 of the Declaration.

²⁵³ This discussed in detail in chapter 4, sec. 3 & 4; *Abacha v Fawehimi* (2000) 6 NWLR (Pt. 660) 228-International law that has been domesticated in Nigeria takes precedence over other statutes.

²⁵⁴ The above discussion argues that the ACtHR has jurisdiction to adjudicate on the right to privacy even though the ACHPR does not provide specifically for the right.

There is no guidance in the ACHPR or from the ACtHR on the regulation of communications surveillance in Africa. The 2019 Declaration remedies this defect by providing for the protection of the right to privacy and specifically data privacy. It also provides guidelines for the regulation of communications surveillance. These guidelines are however broad and have yet to be applied to domestic laws by the ACtHR.

2.4 African sub-regional laws on the right to privacy

This section discusses sub-regional laws protecting the right to privacy that relates to Nigeria and South Africa. These are the Southern African Development Community Model Law on Data Protection, 2013 (SADC Data Protection Law) which relates to South Africa and other Southern African countries that are Member States of SADC and the Supplementary Act on Personal Data Protection within the Economic Community of West African States, 2010 (ECOWAS Data Law) which relates to Nigeria and other West African States.

2.4.1 The Supplementary Act on Personal Data Protection within the Economic Community of West African States 2010

The ECOWAS data law aims to provide legislative guidance to Member States for the laws protecting data privacy.²⁵⁵ It also aims to harmonise the domestic law among ECOWAS Member States on the processing, collection, transmission, storage and use of personal data.²⁵⁶ The ECOWAS data law is an annexure to the ECOWAS treaty and was signed by all Heads of State and Governments of the ECOWAS States, including Nigeria. The ECOWAS data law provides guiding principles for the lawful processing of personal data and also serves as a model law that may be adapted by its Member States in regulating the processing of personal data.²⁵⁷

Article 6 of the ECOWAS data law provides that processing of personal data by or on behalf of the State must be regulated by law. No guideline is provided for the contents of the law that will ensure that the right to privacy is protected adequately during the processing of personal data by the State. It simply suffices that the State formulates a

²⁵⁵ ECOWAS, Supplementary Act on Personal Data Protection within ECOWAS, Feb. 16, 2010, ECOWAS A/SA.JO1/10; Article 2 of the ECOWAS Data Law; Iwobi "Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime" 2016 26 *Transnational Law and Contemporary Problem* 34.

²⁵⁶ *Ibid.*

²⁵⁷ Article 23 of the ECOWAS Data Law.

law to regulate the processing of personal data. The domestic law also does not need to be a statute. This means that the State may formulate a regulation that provides little or no protection for the right to privacy. Unfortunately, the provision of article 6 of the ECOWAS Data law does not provide valuable guidance for Nigeria on the protection of personal data when the State is executing communications surveillance.

2.4.2 Southern African Development Community model law on data protection

The SADC is an inter-governmental organisation that aims to achieve development, peace, security and economic growth in Southern Africa.²⁵⁸ The SADC transformed from a development coordinating conference established in 1980 into a sub-regional economic community in 1992 and currently comprises 16 Member States.²⁵⁹ The SADC Treaty which was signed and opened for ratification in 1992 fostered the creation of the SADC.²⁶⁰ The SADC Treaty provides the legal framework for the SADC and addresses matters such as the aims and objectives of the Treaty, its institutions, financial issues and dispute settlement among its Member States.²⁶¹ South Africa ratified the SADC Treaty in 1994, signifying its intention to be subject to the supranational authority of the SADC Treaty, its protocols, regulatory and judicial authority.²⁶² One of the SADC Treaty's underlying principles is a commitment towards human rights, democracy and the rule of law.²⁶³

Article 4 of the SADC Charter provides that Member States shall adhere to the principles of human rights.²⁶⁴ Article 16 of the SADC Treaty provides for the establishment of the SADC Tribunal which was thereafter established by the Protocol to the SADC treaty.²⁶⁵ The SADC Tribunal, until its suspension in 2011, had the

²⁵⁸ Article 1 of the SADC Treaty.

²⁵⁹ The Southern African Development Co-ordination Conference was established in 1980 by the governments of Angola, Botswana, Lesotho, Malawi, Mozambique, Swaziland, Tanzania, Zambia and Zimbabwe. The SADC was formed in Lusaka, Zambia, on 1 April 1980, following the adoption of the Lusaka Declaration (1980) by the nine founding Member States.

²⁶⁰ The SADC Treaty was signed at Windhoek, Namibia on 17 August 1992, entering into force on 30 September 1993.

²⁶¹ *Ibid.*

²⁶² Saurombe "The Role of SADC Institutions in Implementing SADC Treaty Provisions Dealing with Regional Integration" 2012 15 *Potchefstroom Electronic Law Journal* 455.

²⁶³ Other principles provided for in Article 4 of the SADC Charter are: sovereign equality of all Member States; solidarity, peace and security; equity, balance and mutual benefit; peaceful settlement disputes.

²⁶⁴ Article 4 (c) SADC Charter.

²⁶⁵ The Protocol on the SADC Tribunal entered into force in 2001; The SADC Tribunal was established under the SADC Treaty in 2000 and inaugurated in November 2005

competence to consider individual complaints on human rights violations.²⁶⁶ As a result of the SADC Tribunal's mandate to consider individual complaints on human rights violations, individuals from SADC Member States can seek remedies for infringements on their right to privacy.

The SADC Tribunal, relying on Article 27 of the Vienna Convention, in *Mike Campbell v The Republic of Zimbabwe* stated that the "respondent cannot rely on its national law...to avoid its obligation under the treaty".²⁶⁷ Also, Article 21(b) of the SADC Charter provides for the application of "general principles and rules of public international law". Consequently, even when a national law does not domesticate some international obligations, cases referred to the SADC Tribunal will still be decided on the basis of the national law and the treaties to which the Member State is a party. SADC Member States cannot therefore rely on the absence of the protection of the right to privacy in its national laws to avoid international obligations, like the protection of the right to privacy provided by the ICCPR.

Another function of the SADC is the preparation of model laws providing guidelines on the regulation of particular issues. Model laws in regional organisations are formulated to assist Member States in enacting their domestic legislation and in addition to promote harmonisation of laws within the region.²⁶⁸ Member States have the discretion to adapt these model laws to suit their specific circumstances while maintaining the underlying principles of such models. Model laws are useful in developing standards of regulating new societal challenges affecting several nations. One such issue is the privacy challenges occasioned by the rapid and constant advancement in ICT. These privacy issues have persisted for decades and they require attention by regional organisations in order to ensure harmonised legislation that provides adequate protection for the right. However, only data privacy has been recognised sufficiently to prompt the preparation of a model law in SADC and is known as the SADC Model Law on Data Protection (SADC Data Protection Law).

²⁶⁶ Article 16(1) of the SADC Charter; Article 15 of the Protocol on the SADC Tribunal; The South African Constitutional court declared the suspension of the SADC Tribunal unconstitutional in *Law Society of South Africa v President of South Africa* 2019 (3) BCLR 329 (CC).

²⁶⁷ SADC (T) Case No. 2/2007; *Chimexpan v Tanzania* Case No. SADC (T) 01/2009, Main Decision on June 2010.

²⁶⁸ Viljoen "Model Legislation and Regional Integration: Theory and Practice of Model Legislation Pertaining to HIV in the SADC" 2008 41 *De Jure* 384.

Article 1 of the SADC Data Protection Law defines data as any representation of information regardless of medium or format. This signifies that information acquired before, during and after communications surveillance qualifies as data. Article 1 of the SADC Data Protection Law also defines personal data as any data relating to a data subject. Any data that relates to an identifiable person is referred to as personal data in the SADC Data Protection Law. Information obtained from communications surveillance relates to an identifiable person and protected under the SADC Data Protection Law. The execution of communications surveillance is, however, not provided for in the Law. Nevertheless, article 42 of the SADC Data Protection Law recognises that the duty of the State to protect national security, defence, public safety and/or the prevention of crime may require that certain data protection rights of a data subject be limited. Article 42 of the SADC Data Protection Law permits the exemption of a Member State from the obligation imposed by articles 11(1), 12, 13, 21, 22, 31, 32 and 33 of the SADC Data Protection Law on data controllers, if the processing of such data is for the purpose of preserving defence, national security, public safety and the prevention of crime.²⁶⁹

The activities of SADC Member States when processing personal data obtained from communications surveillance should be guided by article 42. This is however not always the case. For example, the Protection of Personal Information Act (POPIA)²⁷⁰ exempts the South African State from the duties imposed by the Act when processing personal information for national security purposes. Article 42 of the SADC Data Protection Law provides for a limitation of the rights of the data subject by the State and not an exemption from the preservation of the right. The exemption in the POPIA is problematic as the processing of the personal information of a person for national security purposes is not protected by legislation in South Africa. This is discussed in detail in chapter three.²⁷¹

²⁶⁹ Article 11(1) of the SADC Law provides for the principles of data processing such as adequacy, relevance, accurate and the form of retention of data; Article 12 of the SADC provides for the principles of fair and lawful processing of data; Article 13 of the SADC provides for the principle of legitimacy of use of personal data; Articles 21 and 22 of the SADC Law provides for the obligation of the data controller to notify the data subjects of the collection of their personal data; Articles 31-33 of the SADC Data Law provides for the right of the data subjects to access their personal data and request rectification, deletion and/or temporary limitation of access to their personal data.

²⁷⁰ S.6(c) of the Protection of Personal Information Act 4 of 2013.

²⁷¹ Chapter 3, sec. 3.8.3.

2.4.3 Justification for the study of European regional law

The discussion above indicates that the African sub-regional law provides very little guidance for regulating communications surveillance. As a result, it is necessary to look beyond the region to Europe where the right to privacy is recognised in regional conventions. The justification for choosing the European regional law over other regions is that the European regional courts have developed minimum requirements for regulating communications surveillance. These minimum requirements have been developed by testing the domestic laws of various European countries. The relevant decisions have spanned over 10 years with the most recent being *Bigbrother Watch v UK* in 2018. In this case the ECHR explored the intricacies of regulating communications surveillance in great depth.²⁷² It is therefore an excellent example for guidance on regulating communications surveillance in Nigeria.

Furthermore, the OHCHR also relies heavily on the decisions of the European regional courts in its annual report to the Human Rights Council on the “Right to Privacy in the Digital Age”.²⁷³ This may be because the region’s jurisprudence on communications surveillance is more advanced than that in other regions. The European regional courts’ minimum requirements are beneficial to Nigeria and will be contextualised in chapter five to provide recommendations for her communications surveillance regulation regime.

2.5 European regional laws on communications surveillance

Europe, unlike Africa, has more than one regional institution providing a coalition of the European countries and there are several treaties emanating from these regional institutions. For the purpose of this thesis, the discussion focuses on the human rights treaties of the Council of Europe (CoE) and the European Union (EU). This section discusses the European Convention on Human Rights (ECHR) and the EU Charter on Fundamental Rights (the EU Charter). The discussion focuses specifically on the decisions of the European regional courts on communications surveillance.

²⁷² Applications Nos. 58170/13, 62322/14 and 24960/15, Judgment on 13 September, 2018.

²⁷³ Annual report of the Office of the High Commissioner for Human Rights on the Right to Privacy in the Digital age, 28th session, agenda items 2 and 3, A/HRC/28/39, 19 December 2014 par [27].

2.5.1 European Convention on Human Rights

The European Convention on Human Rights (ECHR) is the human rights treaty of the Council of Europe (CoE). The ECHR also establishes and defines the jurisdiction of the ECtHR.²⁷⁴ The mandate of the ECtHR is to consider the application of the domestic laws of the Contracting States and not review the laws *in abstracto*. This means that the ECtHR will only adjudicate on matters that indicate a specific violation of human rights.²⁷⁵ The ECtHR will therefore not adjudicate on matters that aim to review the domestic law of a Contracting State without an alleged infringement on at least one of the rights in the ECHR. Nonetheless, the ECtHR will not require concrete proof of communications surveillance from a claimant.²⁷⁶ The clandestine nature of communications makes it very difficult to prove its occurrence hence the existence of a domestic law regulating the process is usually regarded as sufficient proof of surveillance.²⁷⁷

Regarding communications surveillance, most of the Contracting States of the CoE have domestic laws regulating its utilisation. However, some of these laws, for example the Russian Operational-Search Activities Act²⁷⁸ violate article 8 of the ECHR. The precedent of the European regional courts on communications surveillance discussed in this section and chapter five indicate that the focus of the court has been on the quality, not the existence, of the laws in light of article 8 of the ECHR and other international human rights instruments such as the ICCPR.

Article 8 of the ECHR provides as follows:

²⁷⁴ The ECHR was adopted on 4th November 1950 and entered into force on 3rd September 1953; The founding members of the Council of Europe were Belgium, Denmark, France, Ireland, Italy, Luxembourg, the Netherlands, Norway, Sweden and the United Kingdom (“UK”). Greece, Iceland, Turkey and West Germany became members shortly after the establishment of CoE. The ECHR was originally known as “the Convention for the protection of Human Rights and Fundamental Freedoms”. Presently, 47 States have acceded to the Convention including all Member States of the EU; Article 11 of the ECHR; Granmar “Global Applicability of the GDPR in Context” 2021 11 *International Data Privacy Law* 225.

²⁷⁵ *Zakharov v Russia*, App. No. 47143/06, (2015) par [164]; *Bigbrother Watch v UK* par [398]; Butler and Hidvegi “From Snowden to Schrems: How the Surveillance Debate Has Impacted US-EU Relations and the Future of International Data Protection” 2015-2016 17 *Whitehead Journal of Diplomatic & International Relations* 71.

²⁷⁶ *Zakharov v Russia* par [171]; *Kennedy v United Kingdom*, App. no. 26839/05 (18 May 2010) par [124].

²⁷⁷ *Association for European Integration and Human Rights and Ekimdzhiiev v Bulgaria* par [69]; *Klass v Germany* par [41]; *Malone v United Kingdom* par [64]; *Weber and Saravia v Germany* par App. no. 54934/00 (2006) pars [77-79].

²⁷⁸ 12 August 1995, no.144-FZ; Also, the Code of Criminal Procedure of 18 December 2001, no.174-FZ (in force since 1 July 2002).

1. “Everyone has the right to respect for his private and family life, home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the right and freedom of others.”

Although article 8 of the ECHR provides for the right to privacy, it does not specifically use the word privacy. Instead, the term “private life” is used and has been interpreted by the ECtHR as encompassing the broader right to privacy.²⁷⁹ Article 8(1) of the ECHR also protects correspondence which is “often understood as the right to uninterrupted and uncensored communications with others”.²⁸⁰ Hence, the protection of the content of any kind of communication can be classified under the protection of correspondence, while protection of the metadata of electronic communication may be classified under the general protection of private life.²⁸¹

Ultimately, interference with the metadata of a communication and/or the content of the correspondence is prohibited under article 8 of the ECHR. Article 8(2) of the ECHR provides for the permissible limitation for the right to a person’s private and family life, home and correspondence. The ECtHR has interpreted article 8(2) of the ECHR in light of the three requirements for lawful interference with private life. These are whether the interference is in accordance with the law, necessary in a democratic society and pursues a legitimate aim.²⁸²

Communications surveillance interferes with the right to private life and correspondence, which can only be limited by article 8(2) of the ECHR.²⁸³ This signifies that communications surveillance is only permissible when it is in accordance with the law, necessary in a democratic society and for legitimate aims such as protecting national security, public safety and/or the preservation of the economic well-

²⁷⁹ *Pretty v United Kingdom*, App. No. 2346/02, ECHR (Fourth Section), 29 December 2002, 35 EHRR 1; Georgieva 2015 *Utrecht Journal of International and European Law* 115; Novak *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2005) 387.

²⁸⁰ Harris, O’Boyle and Bates *Laws of the European Convention on Human Rights* (2009) 380; Georgieva, 2015 *Utrecht Journal of International and European Law* 115.

²⁸¹ Sinha 2013 *Loyola Law Review* 917; Georgieva 2015 *Utrecht Journal of International and European Law* 116.

²⁸² Article 8(1) and (2) of the ECHR.

²⁸³ Article 8(1) and (2) of the ECHR.

being of the country.²⁸⁴ Legitimate aims in the utilisation of communications surveillance also include the prevention of crime, disorder and/or protection of health, morals, rights and freedom of others.²⁸⁵ The three requirements for permissible communications surveillance in article 8(2) of the ECHR as interpreted by the ECtHR will now be discussed.

2.5.1.1 Communications surveillance being “in accordance with the law”

The ECtHR interprets a communications surveillance regime that is “in accordance with the law” as meaning that communications surveillance must be prescribed by domestic legislation of a Contracting State to the ECHR which must be accessible, clear and foreseeable, must align with the rule of law and must be in line with article 8(2) of the ECHR.²⁸⁶ “Foreseeability” in the context of communications surveillance means that there must be sufficient detail in the legal system of the Member State on the nature of offences that can prompt surveillance.²⁸⁷ The ECtHR further explains that the availability of a domestic law providing for communications surveillance does not fulfil the lawfulness criterion entirely.²⁸⁸ Domestic laws must therefore provide safeguards against arbitrariness and ensure adequate protection for human rights to be regarded as lawful in terms of article 8.²⁸⁹

The ECtHR reiterates that communications surveillance by the State can destroy democracy in the guise of defending it, hence the need for safeguards against abuse.²⁹⁰ The ECtHR’s duty in evaluating a Contracting State’s communications surveillance regime is to satisfy itself that there are no loopholes in the domestic legislation that can foster abuse. The ECtHR also acknowledges that the actions of an

²⁸⁴ Loideain “EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era” 2015 3 *Media and Communication* 53; Young “Surfing while Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation” 2004 7 *Yale Journal of Law and Technology* 346.

²⁸⁵ Article 8(1) and (2) of the ECHR.

²⁸⁶ *Malone v UK* par [79]; *Zakharov v Russia* pars [92-95]; *Weber and Saravia v Germany*, par [84].

²⁸⁷ *Zakharov v Russia* pars [244-245]; *Kennedy v United Kingdom* par [159]; *Iordachi v Moldova* 25198/02 (10 February 2009) pars [43-44].

²⁸⁸ *Zakharov v Russia* par [236].

²⁸⁹ *Association for European Integration and Human Rights and Ekimdzhiiev v Bulgaria* par [70].

²⁹⁰ *Klass v Germany*, App. No. 5029/71, (1978) par [49-50]; *Leander v Sweden*, App.No. 9248/81, (1987), par [60]; *Camenzind v Switzerland*, App. No. 21353/93 (1997), par [45]; *Lambert v France* App. No. 46043/14, par [31]; Breyer, “Telecoms data retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR” 2005 11 *European Law Journal* 371; Cannataci, “Working Draft Legal Instrument on Government-Led Surveillance and Privacy”(28 February 2018) https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf (accessed on 2019-10-21) 6.

over-zealous officer cannot be completely ruled out and legislation must curtail such excesses.²⁹¹

The ECtHR provides six minimum safeguards against abuse for which the statute regulating communications surveillance of Contracting States must make provision.²⁹²

These minimum safeguards are the criteria for the determining the quality of the law.²⁹³

The law must provide for:

- The nature of the offence giving rise to an interception order;
- The definition of the category of people liable to have their communications intercepted;
- The limit on the duration of the interception;
- The procedure to be followed after the interception that is examination, storage and utilisation of data obtained;
- The precautions to be taken when communicating data to other parties and;
- The circumstances for deletion or destruction of data obtained from interception of communications.

The ECtHR regularly considers these six minimum requirements to determine the quality of the law on communications surveillance under scrutiny. These requirements ultimately assist the ECtHR in determining whether domestic legislation on communications surveillance provides appropriate measures against abuse. In the absence of any of the above stated minimum requirements, the ECtHR has found such legislation to be incapable of providing adequate safeguards against the abuse of communications surveillance and a violation of article 8(2) of the ECHR.²⁹⁴

2.5.1.2 Communications surveillance must be necessary in a democratic society

The ECtHR's judgments emphasise that interference with private life can only be "necessary in a democratic society" if the process is proportional in the circumstance and there are adequate and effective safeguards against abuse of the process.²⁹⁵

²⁹¹ *Klass v Germany*, par [59].

²⁹² *Association for European Integration and Human Rights and Ekimdzhiiev v Bulgaria* App. No. 62540/00 (2007) par [76]; *Weber and Saravia v Germany* par [95].

²⁹³ *Huvig*, App.No. 11105/84 (1990), par [34]; *Amann v Switzerland*, App. No.27798/95, (2000) par [76]; *Bugallo v Spain*, App. No. 58496/00, (2003) par [30].

²⁹⁴ *Bigbrother Watch v UK* nos. 58170/13, 62322/14, 24960/15 (2018); *Bykov v Russia* [GC], no. 4378/02.

²⁹⁵ *Klass v Germany* par [50]; Newell 497, 504.

Once again, the ECtHR introduces the quality of the law as a determinant of whether communications surveillance is necessary in a democracy. This signifies that the quality of the statute regulating communications surveillance is very important in determining compliance with article 8(2).

The actions of the State in respect of the limitation of the right to private life and correspondence in article 8(2) of the ECHR are subject to a test of proportionality during judicial review.²⁹⁶ The ECtHR determines the proportionality of communications surveillance by considering individual cases in their precise circumstances. Thus, there is no “one size fits all” criterion when determining whether communications surveillance is proportional or not.²⁹⁷ However, the ECtHR takes certain factors into consideration when determining proportionality. These include:

“the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law”.²⁹⁸

In addition to proportionality, the ECtHR states that statutes providing for communications surveillance must provide for adequate guarantees against abuse. For this requirement to be met, there must be a competent authority independent of the State that supervises the procedure of communications surveillance.²⁹⁹

2.5.1.2.1 Competent oversight body

The clandestine nature of communications surveillance ensures that surveillance subjects are unaware that they are being monitored unless they are notified. The secrecy of the process signifies that it is highly susceptible to abuse.³⁰⁰ It is important that the supervisory body is both independent from the State and effective to safeguard the surveillance subject against abuse. Legislation must therefore provide for an effective surveillance process that is transparent and minimises the risk of abuse.³⁰¹

²⁹⁶ Jackson “Constitutional Law in an Age of Proportionality” 2015 124 *Yale Law Journal* 3096.

²⁹⁷ *Big Brother Watch v UK* par [309]; Georgieva, 2015 *Utrecht Journal of International and European Law* 122.

²⁹⁸ *Malone v UK* par [81]; *Klass v Germany* par [50]; *Weber and Saravia v Germany* par [106]; *Bigbrother Watch v UK* par [308].

²⁹⁹ *Zakharov v Russia* par [258].

³⁰⁰ *Klass v Germany* par [57]; *Weber and Saravia v Germany* par [135]; *Zakharov v Russia* par [234].

³⁰¹ *Ibid.*

The ECtHR has also held that the review and supervision of communications surveillance takes place before, during and after the surveillance.³⁰² This signifies that the supervision of the surveillance process must commence from the authorisation stage. The authorising body must therefore be independent. The authorising body must also be provided with full access to all relevant information to be capable of scrutinising the application for surveillance.³⁰³ Otherwise, the authorising body will be unable to reach an informed decision.³⁰⁴ The authorising body must also verify that the application for communications surveillance is for one of the legitimate aims that is specified in article 8(2) of the ECHR.³⁰⁵ Additionally, there must be no less restrictive means to achieve the same purpose.³⁰⁶

The ECtHR's guideline in this regard is reflected in its decision in *Weber and Saravia v Germany* where it held that Germany's G 10 Act³⁰⁷ was compliant with the ECHR by virtue of its oversight body. The ECtHR held that the German surveillance regime provided adequate safeguards against abuse as it only permitted surveillance that was "necessary in a democratic society".³⁰⁸ The Court highlighted that the G 10 Act provided for restrictive conditions to be fulfilled before an approval of communications surveillance could be granted and limited surveillance to serious crimes only.³⁰⁹

Furthermore, the G 10 Act details administrative procedure for all stages of communications surveillance. The ECtHR further held that the oversight body for the German's surveillance regime is sufficiently independent.³¹⁰ The G 10 Act's administrative process consists of a G 10 Commission as the authorisation body. The process also involves an independent intermediary who executes the surveillance order. The ECtHR held that the Germany's surveillance regime ensures that communications surveillance was "not ordered haphazardly, irregularly or without due and proper consideration".³¹¹ The decision of the ECtHR was not based on the

³⁰² *Zakharov v Russia* par [233]; *Bigbrother Watch v UK* par [309].

³⁰³ *Zakharov v Russia* par [260]; *Association for European Integration and Human Rights and Ekimdzhiiev v Bulgaria* pars [79-80]; *Zakharov v Russia* par [260].

³⁰⁴ *Ibid.*

³⁰⁵ *Ibid.*

³⁰⁶ *Ibid.*

³⁰⁷ Act of 13 August 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, post under Fernmeldegeheimnisses, "the G 10" Act).

³⁰⁸ *Weber and Saravia v Germany* pars [114-118].

³⁰⁹ *Weber and Saravia v Germany* par [115].

³¹⁰ *Ibid.*

³¹¹ *Ibid.*

transparency of the administrative process for communications surveillance alone, but also because the administrative process had independent supervision.

The G 10 Act provides for a non-judicial authorising body, that is the G 10 Commission which oversees the surveillance procedure and also a Parliamentary Supervisory Board consisting of Members of Parliament.³¹² The ECtHR held that although judicial supervision is desirable in principle, non-judicial bodies that are independent from the State may also be considered appropriate.³¹³ This indicates that the independence of the authorising body and its effectiveness in supervising the surveillance body are the determining factors for an effective oversight body.

Contrasting the Russian surveillance regime with that of Germany, the ECtHR in *Russia v Zakhrov* held the Russian surveillance regime to be non-compliant with the ECHR.³¹⁴ In spite of the Russia's use of the judiciary as the authorising body, the Court held that the oversight body was independent but ineffective because judges had a restricted access to relevant information concerning the surveillance application.³¹⁵ In particular, the judges were unable to scrutinise the applications effectively and make informed decisions.³¹⁶ The ECtHR therefore held that the Russian supervisory body was inadequate to safeguard abuse of the surveillance process and the communications surveillance regime was not "necessary in a democratic society".

2.5.1.2.2 Duration of surveillance

Another determinant of a communications surveillance regime that is necessary in a democratic society is whether the surveillance law provides for a specific duration for the surveillance. The ECtHR held the G 10 Act to be compliant in this regard as it provides for a maximum of three months for the surveillance. A surveillance order expires three months after it is issued.³¹⁷ The Court, however, noted that the provision of the G 10 Act on the transfer of data to other authorities was wide and indeterminate thus constituting "a fairly serious interference" on the right to privacy and which was not compliant with article 8(1) of the ECHR.³¹⁸

³¹² *Ibid.*

³¹³ *Dumitru Popescu v. Romania (no. 2)*, App. No. 71525/01, (2007) par [71]; *Zahkarov v Russia* par [233, 258].

³¹⁴ *Zahkarov v Russia* par [236].

³¹⁵ *Ibid.*

³¹⁶ *Zahkarov v Russia* par [236].

³¹⁷ *Weber and Saravia v Germany* par [116].

³¹⁸ *Weber and Saravia v Germany* par [125].

The ECtHR further held that it is unreasonable to leave the duration of communications surveillance to the State. Legislation must clearly indicate the duration of surveillance.³¹⁹ Furthermore, the domestic legislation of Contracting States must provide for the conditions for cancellation and the extension of surveillance warrants.³²⁰ The absence of any of these requirements in the domestic legislation of a Contracting State signifies that the communications surveillance regime of such State is not necessary in a democratic society.

2.5.1.2.3 An effective avenue for redress

In respect of an effective avenue for the surveillance subject to seek redress, two issues are recurring in the judgments of the ECtHR. They are *locus standi* and post-surveillance notification. On the former, the ECtHR has held that the applicant does not require proof of surveillance to have *locus standi*.³²¹ On the issue of post-surveillance notification, the ECtHR in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* held that the absence of post-notification surveillance in any one instance does not mean that interference is unjustifiable under article 8 of the ECHR.³²² However, failing to notify a surveillance subject of the surveillance cannot be justified where the purpose of the investigation will not be jeopardised by such notification and where there are no other avenues to seek redress.³²³ In respect of both the Bulgarian and Russian legal frameworks on communications surveillance, the ECtHR held that the regimes failed to provide an effective avenue for redress to surveillance subjects and were inconsistent with the ECHR.³²⁴

The ECtHR's position in respect of post-surveillance notification signifies that post-surveillance does not render a surveillance law inconsistent with the ECHR. This

³¹⁹ *Zakharov v Russia* par [250]; *Kennedy v United Kingdom* par [161]; *Klass v Germany* par [52]; *Weber and Saravia v Germany* par [98].

³²⁰ *Ibid.*

³²¹ *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [69]; *Klass v Germany* par [41]; *Weber and Saravia v Germany* pars [77-79]; *Malone v United Kingdom* par [64]; *Liberty v United Kingdom*, App. No. 58243/001 (2008) pars [56-57]; *Iordachi v Moldova* App. No. 25198/02 (2009) par [30-35]; *Zakharov v Russia* pars [165, 168].

³²² *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [90]; *Klass v Germany* par [57]; *Leander v Sweden* App. No. 9248/81 (1987) par [66]; *Weber and Saravia v Germany* par [135].

³²³ *Zakharov v Russia* par [289]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* pars [90-91]; *Dumitru Popescu v Romania* par [77].

³²⁴ *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* pars [91-93]; *Zakharov v Russia* pars [287, 300].

position is reflected in its decisions in *Klass v Germany* and *Kennedy v United Kingdom*.³²⁵ In *Kennedy*, the ECtHR held that the absence of post-surveillance notification in the Investigatory Powers Act (IPA) did not render the Act incompatible with the ECHR.³²⁶ This is because persons who suspect that they are under surveillance can still seek redress with the Investigatory Powers Tribunal (IPT), which is the oversight body for the UK's communications surveillance regime. As a result, the ECtHR held that the IPT at least provided an effective avenue for redress which aligned with the ECHR in spite of the absence of post-surveillance notification.

Similarly, while recognising that the German regime provides for a post-surveillance notification, the ECtHR in *Klass* held that its absence would not have rendered the German surveillance regime inconsistent with the ECHR since there was an effective avenue to seek redress.³²⁷ This avenue for redress is the G 10 Commission, where persons who suspect that they are under surveillance can seek redress.³²⁸ Prior to the ECtHR's adjudication in *Klass*, the applicant had challenged the German surveillance regime at the Federal Constitutional Court which held the absence of post-surveillance notification inconsistent with the German Basic Law.³²⁹ Following the judgment of the Federal Constitutional Court, the German practice in respect of post-surveillance notification is that the Ministers of Defence and of the Interior must continually evaluate, whether a surveillance subject can be notified.³³⁰ The evaluation is based on whether notification can jeopardise the purpose of the surveillance and must then be submitted to the G 10 Commission for a ruling to determine whether the surveillance subject can be notified.³³¹

At the ECtHR, the German's post-surveillance notification approach and its other avenues for redress were considered. The ECtHR highlighted that the German regime provides the surveillance subject with various remedies after the post-surveillance notification. These remedies include an action for a review of the surveillance

³²⁵ *Kennedy v United Kingdom* par [167].

³²⁶ *Ibid*; *Zakharov v Russia* par [288].

³²⁷ *Klass v Germany* par [57].

³²⁸ *Klass v Germany* pars [53, 70].

³²⁹ *Klass*, Collected Decisions of the Constitutional Court, vol. 30, 1, Judgement of 15 December 1970 declaring Article 1(5)(5) of the G 10 Act inconsistent with the German Basic Law to the extent that it does not provide for post-surveillance notification. *Klass v Germany* par [11].

³³⁰ *Klass v Germany* par [19].

³³¹ *Ibid*.

procedure.³³² Also, the surveillance subject may institute an action for damages as a civil law remedy and/or an action for the destruction or restitution of documents.³³³ If unsuccessful, an appeal to the Federal Constitutional Court is available as a last resort.³³⁴ The German surveillance regime thus provides various remedial options for a surveillance subject.³³⁵ For these reasons, the ECtHR held that the German communications surveillance regime provides an effective remedy to surveillance subjects as it combines post-surveillance notification with other avenues for the surveillance subject to seek redress in the event of an unlawful surveillance.³³⁶ **In chapter five of the study, this approach is applied to formulate** reforms for the legal regime of communications surveillance in Nigeria.³³⁷

On the other hand, the ECtHR held that post-surveillance notification is not mandatory and is not recommended for Nigeria for two reasons. First, communications surveillance is executed secretly and it is unlikely that a surveillance subject will suspect surveillance except where there is a leak within process.³³⁸ This should be a concern for the effectiveness of the surveillance procedure employed. Where the procedure is effective, the surveillance subject will not have an opportunity to seek redress. Secondly, the African regional law requires laws authorising communications surveillance to provide post-surveillance notification. Thus, the ECtHR's position does not align with the African regional law.

To summarise, communications surveillance is “necessary in a democratic society” when there is an independent and effective oversight body, the duration of the surveillance is specified in the statute and there are effective remedies available to individuals whom the surveillance law applies.

2.5.1.3 Legitimate aims for communications surveillance

In the context of communications surveillance, it should be noted that there is a difference between communications surveillance being a “necessary means of defence for the protection of a democratic State” and “necessary in a democratic State”. The former refers to the capability of the State to undertake communications

³³² *Klass v Germany* par [71].

³³³ *Ibid.*

³³⁴ *Klass v Germany* pars [24, 71].

³³⁵ *Klass v Germany* par [71].

³³⁶ *Klass v Germany* par [72].

³³⁷ Chapter 5, sec.5.3.2.

³³⁸ *Klass v Germany* pars [55, 68].

surveillance for the sake of her protection especially in light of current threats, including cyber-attacks and cyber-terrorism.³³⁹ The latter, on the other hand, relates to the legitimate aims for which communications surveillance are employed.³⁴⁰ Simply put, although communications surveillance may be necessary to combat crimes, it may only be necessary in a democratic society if its use is justifiable in the circumstances.³⁴¹

The ECtHR has ruled that communications surveillance must only be utilised for legitimate aims specified in article 8(2) of the ECHR. These aims are:

“national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the right and freedom of others.”

Article 8(2) of the ECHR provides a list of reasons under which communications surveillance is permissible. The ECtHR has consistently considered whether communications surveillance is proportionate, given the aim for which it was employed. Thus, the requirements of proportionality and a legitimate aim are often considered together.³⁴²

For example, the ECtHR has only upheld the prevention of serious crimes as legitimate aims where the State is invoking the prevention of disorder and crime as its reasons for communications surveillance.³⁴³ This means that a crime such as pickpocketing is not a legitimate aim for communications surveillance, while counterfeiting money is a legitimate aim only when it is serious enough to affect the economic well-being of the State. If this is not the case, communications surveillance is not considered proportionate. Consequently, communications surveillance is to be used in exceptional situations in line with legitimate aims. In the absence of such exceptional situations, communications surveillance should not be employed as an ordinary means of achieving the daily duties of law enforcement agents.

The ECtHR has the mandate to consider, on a case-by-case basis, the aims listed in legislation of the Contracting States to the CoE in order to determine the legitimacy of

³³⁹ *Digital Rights Ireland v Minister for Communications, Ireland*, App. Nos. C-293/12 and C-594/12 (2014) par [49].

³⁴⁰ *Digital Rights Ireland v Minister for Communications, Ireland* par [51].

³⁴¹ Tzanou, 2010 *Vienna Online Journal on International Constitutional Law* 419.

³⁴² *Kopp v Switzerland* (1998), par [64]; *Valenzuela Contreras v Spain*, App. No. 58/1997/842/1048 (1998) (1998), par [46]; *Malone v UK* par [67]; *Huvig* par [29]; *Weber and Saravia* par [103-106]; *Bigbrother Watch v UK* par [308].

³⁴³ *Zakharov v Russia* par [244].

such aim.³⁴⁴ This is because the aims stated in the limitation clause of the statutes may be interpreted too broadly by the Contracting State. Also, domestic laws of Contracting States on communications surveillance do not provide a definition for terms such as national security, serious crimes, economic well-being and the like. An interpretation from the courts of what constitutes legitimate aims for the purpose of communications surveillance is needed.

Having discussed the minimum standards for legislation on communications surveillance in terms of the ECtHR jurisprudence, the next section discusses the Charter of Fundamental Rights of the EU (the EU Charter) and the Court of Justice of the European Union's (CJEU) decisions on communications surveillance particularly with regard to gathering and storage of meta-data by the State. It should be noted that although the decision of the ECtHR regarding targeted surveillance has remained the same over the years, there have been some changes in respect of bulk surveillance. The ECtHR in *Bigbrother Watch v United Kingdom* reversed its decision in *Weber and Saravia v Germany* to the effect that bulk surveillance is inconsistent with article 8 of ECHR. The court held that innovations in ICT has made bulk surveillance extremely intrusive on privacy compared to when the decision in *Weber and Saravia* was delivered.³⁴⁵

2.5.2 The Charter of Fundamental Rights of the European Union

The EU is also a European international institution with its own treaty on human rights known as the Charter of Fundamental Rights of the EU (the EU Charter).³⁴⁶ The Court of Justice of the European Union (CJEU) is the judicial arm of the EU and is responsible for the interpretation of the EU Charter. The CJEU was established by the Treaty of Paris, 1951 as part of the European Coal and Steel Community and was in existence before the establishment of the EU Charter.³⁴⁷ The CJEU has the duty to

³⁴⁴ *Zakharov v Russia* par [227].

³⁴⁵ The ECtHR in *Bigbrother Watch v UK* App. nos. 58170/13, 62322/14, 24960/15 (2018) par [208].

³⁴⁶ The EU Charter was drafted and adopted in 2000; De Búrca "After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator? 2013 20 *Maastricht Journal of European and Comparative Law* 169.

³⁴⁷ The CJEU was established in 1952 by the Treaty Paris; Tamm "*The History of the Court of Justice of the European Union Since its Origin*" in *The Court of Justice and the Construction of Europe: Analysis and Perspectives on Sixty Years of Case law* (2013) 16.

interpret the EU treaties, ensure compliance of Contracting States to the treaty and review the actions of institutions within the EU.³⁴⁸

Article 7 of the EU Charter provides for the right to privacy. It also identifies everyone's right to the respect of their "private and family life, home and communications". This signifies that the EU recognises the right to privacy as a human right and the Contracting States of the EU are obligated to provide protection for the right to privacy. Also, the CJEU has ruled that any legislation that provides for a generalised surveillance of communications content infringes article 7 of the EU Charter.³⁴⁹

Article 8 of the EU Charter provides for a separate right to personal data as follows:

- “1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by the law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.”

The EU Charter distinguishes the traditional right to privacy in article 7 from the right of personal data in article 8. This distinction signifies that meta-data, being personal data derived from the electronic communications of a person, enjoys distinct protection in the EU Charter.³⁵⁰ Metadata, as explained earlier, is derived from the telephone and/or mobile phone number of a person and such information (metadata) can be used in identifying and even locating a person and therefore, constitutes personal data.³⁵¹ While content data is protected by article 7 of the EU Charter as a component of communications privacy, meta-data is protected in article 8 of the EU Charter as a component of personal data.³⁵²

³⁴⁸ International Justice Resource Center “Court of Justice of the European Union” <https://ijrcenter.org/regional-communities/court-of-justice-of-the-european-union/> (accessed on 2019-03-28).

³⁴⁹ *Schrem v Facebook Ireland Ltd* par [94]; *Digital Rights Ireland v Minister for Communications, Ireland* par [39].

³⁵⁰ Article 2 of Directive 95/46/EC of the European Parliament defines personal data as “any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”

³⁵¹ *Digital Rights Ireland v Minister for Communications, Ireland* par [28].

³⁵² *Ibid.*

As a result of the provision for the right to protection of personal data in article 8 of the EU Charter, the EU has issued several directives on the retention of data. These directives are the Directive 95/46/EC (the 'Data Protection Directive'), the Directive 2002/58/EC (the 'e-Privacy Directive'), the Regulation 45/2001/EC; the Directive 2006/24/EC (the 'Data Retention Directive') and the Council Framework Decision 2008/977/JHA.³⁵³ However, articles 1(2) and 5(2) of Directive 2006/24/EC provide for a lesser protection of meta-data than the content of electronic communications. This illustrates that Directive 2006/24/EC considers the surveillance of metadata as less intrusive than content data which explains the lower statutory protection accorded to the latter.³⁵⁴

The inadequate protection provided for metadata in Directive 2006/24/EC led to the CJEU's decision that articles 1(2) and 5(2) of Directive 2006/24/EC infringes on article 8 of the EU Charter. The CJEU also refers to the minimum standards for communications surveillance developed by the ECtHR as applicable to processing and retention of metadata.³⁵⁵ Since Directive 2006/24/EC did not adhere to the minimum requirements for communications surveillance, the CJEU declared it invalid.³⁵⁶

This discussion on the EU Directives on metadata indicates that for Contracting States in the EU, any regulation on communications surveillance must adhere to the ECtHR's minimum standards. The discussion also signifies that any communications

³⁵³ 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 (OJ) L281 of 23rd November, 1995, 31; 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, OJ L201 of 31st July, 2002, 37; Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L8 of 12th January, 2001,1; Directive 2006/24/EC of the European Parliament and 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 L105 of 13th April, 2006, 54; Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350 of 30th December, 2008,60.

³⁵⁴ *Digital Rights Ireland v Minister for Communications, Ireland* pars [27-31].

³⁵⁵ *Digital Rights Ireland v Minister for Communications, Ireland* par [54]; *Liberty v United Kingdom*, App. No.58243/001, (2008) pars [62-63]; *Rotaru v. Romania*, [GC], no. 28341/95, (2000) par [57-59]; *S. and Marper v United Kingdom*, [GC], App. Nos.30562/04 and 30566/04, (2008) par [99]; *M.K. v. France*, App. No.19522/09, (2013), par [35].

³⁵⁶ *Digital Rights Ireland v Minister for Communications, Ireland* pars [55-71].

surveillance regulation by Contracting States of the ECHR and the EU Charter must protect metadata in the same manner in which content data is protected. Article 25(2) of Directive 95/46/EC specifically provides that a third country which receives personal data from the EU must provide adequate protection against misuse of such data.

In interpreting article 25(2) of Directive 95/46/EC, the CJEU's ruled that a person whose personal data is being processed by a third country has the right to seek redress in that country.³⁵⁷ This signifies that if the data of a citizen of any of the Contracting States to the EU is to be processed in Nigeria, such processing must be in line with article 25(2) of the Directive 95/46/EC. If Nigeria is to be involved in the processing of personal data of any citizen of the Contracting State of the EU, Nigerian laws must comply with article 25(2) of Directive 95/46/EC.

Article 8(3) of the EU Charter provides for the independent supervision of the processing of personal data and the European Data Protection Supervisor is designated for that purpose.³⁵⁸ The independence of the supervisory body for communications surveillance is one of the standards that the ECtHR uses to ascertain whether communications surveillance has adequate safeguards against abuse.

Article 52(1)-(3) of the EU Charter provides as follows:

- “1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
2. Rights recognised by this Charter which are based on the Community Treaties or Treaty on European Union shall be exercised under the conditions and within the limits defined by Treaties.
3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.”

Article 52(1) of the EU Charter provides that provision for the limitation of all rights, including the right to privacy, must be made by law. Thus, provision for communications surveillance must also be made by law. Article 52(3) of the EU Charter also provides that rights in the ECHR and the EU Charter that are similar

³⁵⁷ *Schrem v Data Protection Commissioner* App. No. C-362/14, (2015) par [95]; *Digital Rights Ireland v Minister for Communications, Ireland*, pars [47-48].

³⁵⁸ Tzanou, 2010 *Vienna Online Journal on International Constitutional Law* 414.

should be given the same interpretation.³⁵⁹ As a result, the minimum requirements for the regulation of communications surveillance developed by the ECtHR also applies in the CJEU. The CJEU will achieve the same interpretation in relation to communications surveillance by applying the ECtHR's minimum requirements.³⁶⁰

The discussion on the CJEU's interpretation of article 7 and 8 of the EU Charter signifies that the EU Charter's protection of personal data is not subsumed in the general right to private life like article 8 of the ECHR. The discussion also indicated that the CJEU has more developed precedent on the protection of personal data. However, with regard to the regulation of communications surveillance, the ECtHR's interpretation of article 8 of the ECHR is more developed. It also provides valuable assistance for the reforms needed to the Nigerian legal framework on communications surveillance so as to ensure the protection of the right to privacy.

2.6 Conclusion

The discussion in this chapter indicates that the international law on communications surveillance includes general guidelines on the interference with privacy, the family home, correspondence and communications. However, there are no minimum requirements that set out the exact contours for a statute on communications surveillance that is both lawful and non-arbitrary.

Also, the definitions of the terms "unlawful" and "arbitrary" are scattered throughout several UN reports and resolutions. These reports and resolutions are merely persuasive documents and do not provide authoritative guidance to Member States of the required standard for statutes regulating communications surveillance. It is therefore suggested that the Human Rights Council collate the principles in General Comment 16 of the ICCPR, UN resolutions and reports into a new General Comment or Resolution to guide Member States.

The discussion in section 2.1.2 shows that the Human Rights Council has tried to apply article 17 of the ICCPR and General Comment 16 to current issues of privacy in the

³⁵⁹ European Convention for the Protection of Human Rights and Fundamental Freedoms was the initial name of the ECHR.

³⁶⁰ *Nowak v Data Protection Commissioner*, App. No. C-434/16 (2017); *Schrems v Facebook Ireland Ltd* App. No C-498/16 (2018); *Google Spain v Google* C-131/12 (2014); *GC v CNIL* App. No. C-136/17(2019); *Digital Rights Ireland v Minister for Communications, Ireland; Secretary of Home Department v Watson* App. No. C-201/15 and C-698/15 (2018); *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* EU Official Journal, App. No. C22 22/1/18 29-30 (2017).

digital sphere. As a result, broad guidelines for the legitimate interference with privacy, family, home, correspondence and communication have been developed. In summary, these are:

- The domestic law of a Member State must prescribe interference with privacy, family, home, correspondence and communication. Such domestic law must be of general application, clear, precise, publicly accessible and non-discriminatory;
- Any interference with privacy, home, family, correspondence and communication must be reasonable;
- The domestic law regulating interference with privacy, home, family, correspondence and communication must specify the precise circumstance of such interference;
- The domestic law regulating interference with privacy, home, family, correspondence must provide for the designated authority that authorises interference with privacy;
- The domestic law regulating interference with privacy, home, family, correspondence must also provide that the decision to permit such interference should occur on a case-by-case basis; and
- Communications surveillance may only be utilised for legitimate purposes recognised in international law.

African regional law, in particular, the 2019 Declaration, provides guidance for the regulation of communications surveillance. The principles in the 2019 Declaration are however broad and do not provide adequate guidelines to AU Member States as to when privacy is to be limited. The principles in the 2019 Declaration are similar to the guidance provided by international law. The sub-regional laws discussed provides guidance in respect of data privacy only. It therefore only applies to the protection of personal data acquired from communications surveillance.

The European regional law on communications surveillance is well developed and provides minimum requirements for the statutory regulation of communications surveillance for their Contracting States. Furthermore, the HRC in its rulings on communications surveillance has made several references to the cases decided by European regional courts. The minimum requirements on communications

surveillance as developed by the ECtHR will therefore be utilised alongside the standards set by international law to measure the adequacy of statutes regulating communications surveillance. These requirements will also be applied to the development of Nigeria's law. They are that laws must provide for: the nature of offence that can prompt surveillance and define category of persons that can be subjected to surveillance; the duration of surveillance; post-surveillance processing of information; precautions to be taken when surveillance information is transferred and; the circumstance for the destruction of surveillance information.

Before moving to Nigeria, however, the protection of the right to privacy and the regulation of communications surveillance in South Africa is analysed. This is done to provide a domestic comparator for Nigeria's legal framework.

CHAPTER THREE
AN ANALYSIS OF THE LEGAL FRAMEWORK OF COMMUNICATIONS
SURVEILLANCE IN SOUTH AFRICA

3.1 Introduction

This chapter assesses the manner in which communication surveillance is regulated in South Africa in order to provide guidance for the development of the Nigerian law.

The previous chapter examined the international standard for the regulation of the interference with the right to privacy. It also highlighted the minimum requirements for a communications surveillance regulation regime that is lawful and non-arbitrary. The European Court of Human Rights (ECtHR) decisions discussed revealed that adequate safeguards are needed to ensure that the rights of surveillance subjects are not arbitrarily infringed. As highlighted in chapter one, Nigeria's regulatory framework for communications surveillance provides minimal safeguards for the right to privacy. For Nigeria to develop a lawful and non-arbitrary legislative framework to regulate communications surveillance, it is necessary to draw lessons from other regimes with more advanced jurisprudence on the right to privacy.

The right to privacy is the main right impacted by communications surveillance. Privacy jurisprudence is thus crucial in the development of the law relating to communications surveillance. South Africa has ratified the International Covenant on Civil and Political Rights (ICCPR) and has an obligation to ensure that the utilisation of communications surveillance is regulated by national law.³⁶¹ In South Africa, the right to privacy is protected by the Constitution, the common law and statute.³⁶² Communications surveillance is regulated either generally through the Constitution and the common law's protection of privacy or specifically through statutes such as the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA),³⁶³ the Cybercrimes Act,³⁶⁴ the Electronic Communications and

³⁶¹ Neethling and Potgieter *Law of Delict* 8ed (2021) 18.

³⁶² Burchell "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid" 2009 13 *Electronic Journal of Comparative Law* (EJCL) 2; Van der Walt and Midgley (eds) *Principles of Delict* 4ed (2016) 6.

³⁶³ The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

³⁶⁴ The Cybercrimes Act 19 of 2020.

Transaction Act (ECTA)³⁶⁵ and the Protection of Personal Information Act (POPIA).³⁶⁶ These laws will be analysed to assess the available safeguards for the protection of rights while executing communications surveillance in South Africa.

The discussion in this chapter also highlights the effectiveness of communications surveillance through the criminal justice procedure. It further emphasises that the unlawful and arbitrary utilisation of communications surveillance contributes to the erosion of a democracy. The regulation of communications surveillance should thus be focused on the protection of human rights as opposed to how its utilisation can be enabled.

The chapter commences by drawing parallels between Nigeria and South Africa to show the relevance of South Africa's jurisprudence for the development of the Nigerian law. Thereafter, the South African jurisprudence on privacy is considered, starting from the Constitution and moving to the common law to establish the protection afforded to the right to privacy and its legitimate limitations. The manner in which the Constitution and the common law work together to protect the privacy of persons in South Africa is then analysed.

The chapter further examines the statutory regulation of communications surveillance in South Africa and analyses its compliance with the Constitution. It also discusses the decision of the Constitutional and High Court in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services*³⁶⁷ which declared some of the provisions in the RICA unconstitutional on five grounds.³⁶⁸ The AmaBhungane case involved the interception of the communications of an investigative journalist, Sam Sole, and a state prosecutor Billy Downer.³⁶⁹ The interception of their electronic communications was revealed during the investigation into the former President, Jacob Zuma, alleged corruption. Zuma's attorney attached the transcripts of the intercepted communication to the court papers. The interception

³⁶⁵ The Electronic Communications and Transactions Act 25 of 2002.

³⁶⁶ The Protection of Personal Information Act 4 of 2013; S. 39(1) of the Constitution; Neethling and Potgieter *Law of Delict* (2021) 18.

³⁶⁷ *AmaBhungane v Minister of Justice* 2020 (1) SA 90 (GP) {*AmaBhungane v Minister of Justice* (GP)}; *AmaBhungane v Minister of Justice* 2021 (4) BCLR 349 (CC) {*AmaBhungane v Minister of Justice* (CC)}.

³⁶⁸ Chapter 3, sec. 3.8.2.5.1.

³⁶⁹ Global Freedom of Expression, Columbia University "*Amabhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services*" <https://globalfreedomofexpression.columbia.edu/cases/amabhungane-centre-for-investigative-journalism-v-minister-of-justice-and-correctional-services/> (accessed 2023-01-28).

was executed under the RICA, with the AmaBhungane, Sole's employer, then challenging the validity of the law.

The chapter concludes by summarising the recommendations to guide Nigeria's communications surveillance regime. These are then applied to Nigeria in subsequent chapters, taking cognisance of the differences between the constitutional provisions on the right to privacy and its limitations.

3.2 Importance of South African jurisprudence to the study and the links between South Africa and Nigeria

South Africa has a rich privacy jurisprudence. South Africa is also a Member State of the United Nations and, like Nigeria, has an obligation to ensure adequate protection for the right to privacy. This obligation on States, as discussed in chapter two, includes ensuring that the utilisation of communications surveillance does not unlawfully and arbitrarily interfere with the right to privacy and other rights.³⁷⁰ South Africa, aside from also being an African country, suffered oppression under the apartheid regime. Hence, South Africa's Constitution is committed to the eradication of oppression and to ensuring that arbitrary surveillance practices such as those characterised by the apartheid government are not repeated.³⁷¹

Having survived various military dictatorships, Nigeria also has similar interests. The scars from the past are still fresh in the minds of citizens of both countries. It is beneficial for Nigeria to learn how South Africa navigates its present constitutional democracy, particularly as regards the right to privacy.³⁷² It is also important to consider South Africa's jurisprudence on the limitation of rights, because this impacts its legislative framework on communications surveillance. This holistic analysis will enable comparative contextualisation and application to Nigeria.

South Africa's regulatory framework on communications surveillance, even though imperfect, is more advanced than that which exists in Nigeria.³⁷³ One reason is that South Africa has a primary statute dedicated to the regulation of communications

³⁷⁰ Chapter 2, sec.2.2.2.5.

³⁷¹ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* (CC) par [26]; *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC) par [25]; Duncan *The Rise of the Securocrats: The Case of South Africa* (2014) 9

³⁷² Duncan *Stopping the Spies: Constricting and Resisting the Surveillance State in South Africa* (2018) 89.

³⁷³ Duncan *Stopping the Spies* 109.

surveillance, namely the RICA.³⁷⁴ This statute was successfully challenged in the High Court in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services (AmaBhungane)* and the decision was confirmed by the Constitutional Court.³⁷⁵

This is unlike the position in Nigeria, where provisions on communications surveillance are contained in various laws. These laws are the Terrorism (Prevention and Prohibition) Act, 2022 (TPPA), Cybercrimes (Prohibition, Prevention, etc) Act, (CPPA), 2015 and the Lawful Interception of Communication Regulation, 2019 (LICR). The TPPA and the CPPA enable the State to execute communications surveillance for the criminal justice procedure relating to terrorism and cybercrimes.³⁷⁶ As stated in chapter four, these statutes enable law enforcement agencies to possess unrestrained use of communications surveillance to perform their objectives. The LICR is the only law that focuses on communications surveillance and it is an inferior law with many problems. It also provides scant protection for human rights. This is addressed in detail in chapter four.³⁷⁷

3.3 Constitutional framework in South Africa

3.3.1 Constitutional values

The South African Constitution is the supreme law of the land and all other laws derive their validity from it.³⁷⁸ The South African Constitution is interpreted in light of its foundational values.³⁷⁹ The duty of the courts, when asked to develop or interpret the law, is to “articulate the unfulfilled obligation [of Parliament] in broad terms, but with sufficient clarity to give Parliament a fair sense of what is required of it...in developing

³⁷⁴ Act 70 of 2002.

³⁷⁵ 70 of 2002; *AmaBhungane v Minister of Justice* (GP) par [67]; *AmaBhungane v Minister of Justice* (CC) par [157].

³⁷⁶ S.1(a) of the TPPA. The preamble to the Terrorism (Prevention and Prohibition) Act provides for its objective as “[a]n Act to make provisions for and about offences relating to conduct carried out or purposes connected with terrorism”.

³⁷⁷ Chapter 4, sec.4.9.4.3.

³⁷⁸ S.2 of the Constitution.

³⁷⁹ S.1 of the Constitution provides that the foundational values of the Republic of South Africa are human dignity, advancement of rights and freedoms, supremacy of the Constitution and the rule of law.

a fitting regulatory framework”.³⁸⁰ In so doing, the courts also guard and enforce the underlying values of the Constitution.³⁸¹

The interpretation of laws must reflect these constitutional values.³⁸² In the same vein, the interpretation of the Bill of Rights must “promote the values that underlie an open and democratic society...”³⁸³ Some of the underlying values are specifically important for the regulation of communications surveillance so that it does not become a tool for subverting democracy. The regulation of communications surveillance must, therefore, be such that it reflects constitutional values that uphold a democratic government. These values are legality, openness, and accountability, which can be used to temper the inherent secrecy of the communications surveillance process to protect human rights.³⁸⁴ These values are also important components of the international law requirement of lawfulness and non-arbitrariness for national laws limiting the right to privacy.³⁸⁵ Legislation that aligns with the Constitution and international law must therefore reflect these values at all stages of communications surveillance.

3.3.2 Legality of laws in the South African context

Laws that are inconsistent with the Constitution are invalid to the extent of their inconsistency.³⁸⁶ Any provision in legislation that does not align with the Constitution can be referred to a competent authority “to correct the defect”.³⁸⁷ This signifies that

³⁸⁰ *My Vote Counts NPC v Minister of Justice and Correctional Services* 2018 (5) SA 380 (CC) par [76].

³⁸¹ Ss. 38 and 39(1) of the Constitution.

³⁸² S.39(2) of the Constitution; *Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Tourism* 2004 (7) BCLR 687 (CC) pars [72-73].

³⁸³ S.39(1)(a) of the Constitution.

³⁸⁴ Ss.1(a)-(d) of the Constitution; *De Klerk v Minister of Police* 2020 (1) SACR 1 (CC) par [69]; Ss. 1(c)-(d), 2 and 41 (1)(c) of the Constitution.

³⁸⁵ Chapter 2, sec.2.2.2.5; *Hulst v Netherland* Communication No. U.N.Doc.CCPR/C/82/D/903/1999 (2004) par [7.7].

³⁸⁶ S.172 (1)(a) of the Constitution; *Minister of Police v Kunjana* 2016 (2) SACR 473 (CC) par [32]. The Constitutional Court declared s.11(1) (a) and (g) of the Drugs and Drug Trafficking Act 140 of 1992 invalid because it was an impermissible violation of the right to privacy; The constitutional interpretation of provisions of the Constitution may change with various developmental stages in the society. Hence, a Constitution cannot be “fossilized”, it must be interpreted consistently by the judiciary. Current developments in ICT and surveillance can be interpreted in light of the Constitution even though such issues were not present at the time of the composition of the Constitution; Ackermann “Constitutional Comparativism in South Africa” 2006 123 *South African Law Journal* 504.

³⁸⁷ *Ibid*; *Islamic Unity Convention v Independent Broadcasting Authority* 2002 (4) SA 294 (CC) par [51]; *Qwelane v South African Human Rights Commission* 2020 (2) SA 124 (SCA) par [96]; *National Coalition of Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC) par [106].

when certain provisions of a law are challenged, the entire law does not have to be nullified. However, where the purpose of the entire statute is to prohibit actions and activities that are constitutionally protected, such a statute will be nullified in its entirety.³⁸⁸

The requirement that laws be consistent with the Constitution also means that actions of law enforcement officers (LEOs) must be supported by laws that align with the Constitution, otherwise such actions will be arbitrary.³⁸⁹ This supports the principle of legality, one of the underlying values of the Constitution,³⁹⁰ and a requirement for any communications surveillance regulation that is compliant with international law.³⁹¹

3.3.3 Openness and accountability

Openness and accountability are underlying constitutional values upon which the South African democratic society is founded.³⁹² These values are aided by the separation of powers.³⁹³ Several rights in the Constitution point to the values of openness and accountability as a foundation upon which a constitutional democracy can stand.³⁹⁴ The aim of the values of openness and accountability is to hold the State

³⁸⁸ *AmaBhungane v Minister of Justice* (GP) pars [53, 68, 89]; *AmaBhungane v Minister of Justice* (CC) par [157]; *South Africa: Constitutional Law Judicial Decisions "Justice Alliance of South Africa v President of the Republic of South Africa 2012 1 LRC 66" 2013 39 Commonwealth Law Bulletin 228.*

³⁸⁹ S.8(1) of the Constitution; *Minister of Police v Kunjana* par [42]; *Estate Agency Affairs v Auction Alliance (Pty) Ltd* 2014 (3) SA 106 (CC) par [40]; *Ngqokumba v Minister of Safety and Security* 2014 (5) SA 112 (CC) par [13]; *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 (1) SA 545 (CC) par [41]; De Villiers "Constitutional Validity of ss.11(a) and (g) of the Drugs and Drug Trafficking-Act: *Minister of Police v Kunjana*" 2017 80 *Journal of Contemporary Roman-Dutch Law* 172.

³⁹⁰ S.172 (2)(a) of the Constitution; *Minister of Police v Kunjana* par [44]; The Constitutional Court in *Pharmaceutical Manufacturers Association of South Africa: In re Ex parte President of the Republic of South Africa* 2000 (2) SA 674 (CC) par [85] stated that "it is a requirement of the rule of law that the exercise of public power by the executive and other functionaries should not be arbitrary."

³⁹¹ The Constitution by virtue of s.39(1)(b) has therefore provided an avenue to reduce unreasonable and unjustifiable infringement of rights.

³⁹² S.1(d) of the Constitution provides that accountability, responsiveness and openness are some of the values upon which the Republic of South Africa is founded; *De Klerk v Minister of Police* par [69].

³⁹³ *Independent Newspaper (Pty) Ltd v Minister for Intelligence Services: In re Masetlha v President of the Republic of South Africa* 2008 (5) SA 31 (CC) par [40]; *De Klerk v Minister of Police* par [170]; *Azanian Peoples Organization (AZAPO) v President of the Republic of South Africa* 1996 (4) SA 671 (CC) par [12]; *Economic Freedom Fighters v Speaker, National Assembly* 2016 (3) SA 580 (CC) par [90].

³⁹⁴ Rights such as access to court and fair trial; *S v Jaipal* 2005 (1) SACR 215 (CC) par [26]; *Bosasa Operations (Pty) Ltd v Basson* 2013 (2) SA 570 (GSJ) par [138]; *AmaBhungane v Minister of Justice* (GP) par [132]; *AmaBhungane v Minister of Justice* (CC) par [93].

responsible for its actions.³⁹⁵ It is difficult to hold the State responsible for activities that are unknown to the public.

Openness and accountability in governance ensure that the powers that are given to the State in terms of the Constitution are not utilised arbitrarily.³⁹⁶ A clear demarcation between the legislature, executive and judiciary is important for ensuring accountability in the utilisation of communications surveillance.³⁹⁷ In the same vein, openness is important for checks and balances among the arms of government. These values are very important for a communications surveillance regulation regime that adequately safeguards rights.

The clandestine nature of communications surveillance makes it prone to abuse.³⁹⁸ Openness and accountability are therefore important at every stage of the surveillance process. For example, the Human Rights Committee (HRC) noted in its report on the South African model of regulating communications surveillance that:

“[t]he State Party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies”.³⁹⁹

One way of achieving this is the creation of an independent oversight body that respects the separation of powers and facilitates openness and accountability in a communications surveillance regime.⁴⁰⁰ The way in which South Africa has balanced the protection of the right to privacy with the need to conduct surveillance is now explored.

³⁹⁵ *Director-General, Department of Home Affairs v Link* 2020 (2) SA 192 (WCC) par [24].

³⁹⁶ *De Klerk v Minister of Police* par [170, 171]; *Economic Freedom Fighters v Speaker, National Assembly* 2016 (3) SA 580 (CC) par [90]; *Azanian Peoples Organization (AZAPO) v President of the Republic of South Africa* 1996 (4) SA 671 (CC) par [12].

³⁹⁷ S.55(2)(a) of the Constitution provides that the National Assembly must provide mechanisms to ensure the accountability of the executive to it; *De Klerk v Minister of Police* par [178]; *Glenister v President of the Republic of South Africa* 2009 (1) SA 671 (CC) par [29] (Glenister I); *South African Association of Personal Injury Lawyers v Heath* 2001 (1) SA 883 (CC) par [22]; Okpaluba “The Constitutional Principle of Accountability: A Study of Contemporary South African Case Law” 2018 33 *Southern African Public Law* 2.

³⁹⁸ *My Vote Counts NPC v Minister of Justice and Correctional Services* pars [45, 47].

³⁹⁹ Report of the United Nations Office High Commissioner for Human Rights “Concluding Observations on the Initial Report of South Africa, CCPR/C/125/3/Add.2, 27 April 2016 pars [42-43].

⁴⁰⁰ *Ibid*; *AmaBhungane v Minister of Justice* (CC) par [90].

3.4 Constitutional protection of the right to privacy in South Africa

Section 14 of the Constitution provides for the protection of privacy in circumstances where there is a subjective expectation of privacy.⁴⁰¹ Section 14 of the Constitution provides as follows:

- "Everyone has the right to privacy, which includes the right not to have—
- (a) their person or home searched;
 - (b) their property searched;
 - (c) their possessions seized; or
 - (d) the privacy of their communications infringed."

Subsections (a)-(d) specify some of the spheres in which society recognises a subjective right to privacy which is objectively reasonable.⁴⁰² The activities specifically mentioned in these subsections are not exhaustive. The term "includes" preceding section 14(a)-(d) connotes that the general right to privacy has a wide ambit. It also suggests that the enumerated list in section 14(a)-(d) is part of the general right to privacy.⁴⁰³ The activities specified in section 14(a)-(d) have been shown to have a higher propensity of infringement by the State.⁴⁰⁴ The privacy of communications falls within this category and it is specifically identified for protection in section 14(d).

Globally, scholars have struggled to define the nature and scope of the right to privacy.⁴⁰⁵ The Constitutional Court's definition of privacy in *Khumalo v Holomisa*⁴⁰⁶ suggests that privacy in the South African context refers to a "sphere of intimacy and autonomy" possessed by human beings and protected against invasion by unauthorised persons.⁴⁰⁷ The Constitutional Court has further stated in *AmaBhungane*

⁴⁰¹ Currie and De Waal *The Bill of Rights Handbook* 6ed (2013) 295.

⁴⁰² *Ibid*; *McKinley Transport Ltd v The Queen* (1990) 68 DLR (4th) 568, 578; *Hunter v Southam Inc.* (1984) 11 DLR (4th) 641 (SCC) 652-653.

⁴⁰³ Currie and De Waal *The Bill of Rights Handbook* 294-295.

⁴⁰⁴ The instances highlighted by the Constitutional Court as examples of wrongful intrusion of privacy under common law are mostly the instances mentioned specifically in s.14(a)-(d); *Bernstein v Bester* 1996 (2) SA 751 (CC) par [67]; *Mistry v Interim National Medical and Dental Council of South Africa* par [8-10]; *Magajane v Chairperson, North West Gambling Board* 2006 (5) SA 250 (CC) par 33; *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division* 2004 (1) SA 406 (CC) par [59]. Burchell "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid" 2009 13 *Electronic Journal of Comparative Law* 12.

⁴⁰⁵ Solove "I've Got Nothing to Hide' and other Misunderstandings of Privacy" 2007 44 *San Diego Law Review* 745; McCreary "What Was Privacy?" 2008 86 *Harvard Business Review* 123; Neethling "The Right to Privacy, HIV/AIDS and Media Defendants" 2008 36 *South African Law Journal* 37; Solove "Understanding Privacy" 2008 *The George Washington University Law School Public Law and Legal Theory Working Paper No.420* 8; DeCew *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (1997) 1.

⁴⁰⁶ 2002 (5) SA 401 (CC) par [27].

⁴⁰⁷ *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg v Minister of Police* 2022 (1) BCLR 46 (CC) par [41]; *Bernstein v Bester* par [65]; Warren and Brandeis "The Right to Privacy" 1890 (4) *Harvard Law Review* 205.

that the protection of the right to privacy also advances the protection of the right to dignity, which is, reflective of a free and democratic society.⁴⁰⁸

Neethling describes privacy “as a condition of human life characterized by seclusions from the public and publicity. This implies an absence of acquaintance with the individual or his personal affairs in this state”.⁴⁰⁹ Neethling’s definition was based on the common law concept of privacy. In *Bernstein v Bester* Ackermann J expounded on Neethling’s definition in light of the Interim Constitution and introduced the notion of a reasonable expectation of privacy.⁴¹⁰

The notion of a legitimate expectation of privacy plays an important role in the evaluation of the scope of the constitutional right to privacy in South Africa.⁴¹¹ A subjective expectation of privacy acknowledged by society as being objectively reasonable must exist.⁴¹² The decisions of the Constitutional Court on the right to privacy use this reasoning. Reasonableness is measured in terms of a continuum of privacy interests.⁴¹³ The level of protection afforded a person varies by whether the action took place in an inner sanctum.⁴¹⁴

The Constitutional Court in *Bernstein v Bester* held that:

“A high level of protection is given to the individual’s intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual’s activities then acquire

⁴⁰⁸ *AmaBhungane v Minister of Justice* (CC) par [28]; *Khumalo v Holomisa* par [27]; *Thomas v Minister of Home Affairs* 2000 (8) BCLR 837 (CC) par [35]; *S v Makwanyane* 1995 (3) SA 391 par [328]; *President of the Republic of South Africa v Hugo* 1997 (4) SA 1 (CC) par [41].

⁴⁰⁹ Neethling and Potgieter *Law of Delict* 422; Neethling “The Concept of Privacy in South African Law” 2005 18 *South African Law Journal* (SALJ) 19; See also *National Media Ltd v Jooste* 1996 (3) All SA 262 (A) 270-272; *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) at 462F; *Bernstein v Bester* par [65].

⁴¹⁰ Neethling “The Concept of Privacy in South African Law” 2005 18 *South African Law Journal* (SALJ) 19; See also Warren and Brandeis “The Right to Privacy” 1890 (4) *Harvard Law Review* 205; Currie and De Waal *The Bill of Rights Handbook* 298; *Bernstein v Bester* par [75]; *Khumalo v Holomisa* par [27].

⁴¹¹ *Bernstein v Bester* par [68]; *United States v Dionisio* 420 US 1 (1975) 14; *United States v Mara* 410 US 19 (1973) 21; *Katz v United States* 389 US 347 (1967) 361; *Abel v United States* 362 US 217 (1960) 241.

⁴¹² *Bernstein v Bester* pars [75-78]; Currie and De Waal *The Bill of Rights Handbook* 297-298.

⁴¹³ *Bernstein v Bester* par [75].

⁴¹⁴ *Bernstein v Bester* par [67].

a social dimension and the right of privacy in this context becomes subject to limitation.”⁴¹⁵

The concept of spheres of privacy was introduced in *Bernstein v Bester*, when distinguishing spheres of privacy where an exclusive expectation of privacy is reasonable.⁴¹⁶ Different levels of protection are afforded to persons when they are in their intimate sphere and when they exit that intimate sphere.⁴¹⁷ The inner sanctum represents facts that are in the “truly personal realm” and is protected exclusively but not absolutely.⁴¹⁸ Intimate facts that are protected by individuals from the public realm also qualify as inner sanctum and these include home and its environment, family life, sexual preference and personal life.⁴¹⁹

The Constitutional Court also defined the spheres considered as inner sanctum in *Bernstein v Bester* as follows:

“In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community.”⁴²⁰

The right to privacy being interpreted as the protection of inner sanctum from external intrusion is intended to give persons exclusive, not absolute, control over spaces legally recognised as inner sanctums.⁴²¹ The exclusive control of private spheres is not an unrestrained permission to do as one pleases, irrespective of whether one is perpetrating an unlawful act.⁴²² Rather, it indicates that prohibitions which invade the inner sanctum will limit the right to privacy. The prohibitions must then be justified in terms of section 36 of the Constitution.⁴²³

Even though the objectives of the right to privacy are to protect people and not places, certain spaces such as the home are reserved for “the most private of activities”.⁴²⁴

⁴¹⁵ *Ibid.*

⁴¹⁶ *Bernstein v Bester* par [77].

⁴¹⁷ *Prince v Minister of Justice* 2017 (4) SA 299 (WCC) par [22]; *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC) pars [27-29]; *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) v Smit* pars [17-18].

⁴¹⁸ *Bernstein v Bester* par [67]; *Centre for Child v Media 24 Ltd* 2020 (1) SACR 469.

⁴¹⁹ *Ibid.*; *NM v Smith* 2007 (5) SA 250 (CC) par [27]; *Mistry v Interim Medical and Dental Council of South Africa* par [27].

⁴²⁰ *Bernstein v Bester* pars [65-67]; *Estate Agency Affairs Board v Auction Alliance (Pty) Ltd* 2014 (4) BCLR 373 (CC) par [34].

⁴²¹ *Minister of Justice and Constitutional Development v Prince* 2019 (1) SACR 14 (CC) par [52]; *AmaBhungane v Minister of Justice* (CC) par [24]; Neethling 2005 18 SALJ 21.

⁴²² *National Coalition of Gay and Lesbian Equality v Minister of Justice* par [118].

⁴²³ *Minister of Justice and Constitutional Development v Prince* par [58].

⁴²⁴ *Mistry v Interim Medical and Dental Council of South Africa* par [28].

Protecting those spaces equates protecting the privacy of the individuals involved in those activities. Therefore, the right to privacy of persons is ultimately protected when objects, such as mobile phones and computers that store very intimate information about persons, are protected from unauthorised intrusion.⁴²⁵

The interpretation of privacy by the Constitutional Court signifies that privacy involves a personal autonomy in which a person is capable of excluding intrusion from outsiders.⁴²⁶ However, the constitutional protection of the inner sanctum of privacy does not mean protection is afforded absolutely. It merely indicates that the intimate sphere is “shielded from erosion by conflicting rights of the community”.⁴²⁷ There is a lower level of protection for information or facts in the public realm.⁴²⁸

To illustrate the different levels of review for public and private spaces, in *Minister of Constitutional Development v Prince*, the Constitutional Court was required to assess the constitutionality of the Drugs and Drug Trafficking Act and Medicine and Related Substances Control Act, which prohibited the smoking of cannabis.⁴²⁹ The Constitutional Court agreed with the statutory prohibition of the use of cannabis in public spaces because of the health risks to non-smokers.⁴³⁰ The contentious issue was the prohibition of the growing and use of cannabis “where the possession, purchase or cultivation of cannabis is for personal consumption by an adult” in a private dwelling.⁴³¹ The Constitutional Court confirmed that the criminalisation of growing and use of cannabis in private spaces was inconsistent with the constitutional right to privacy and different standards of justification are applicable to private spheres

⁴²⁵ S.6 of 19 of 2020 prohibits the unlawful interference with computer systems.

⁴²⁶ *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1998 (12) BCLR 1517 (CC) par [32]; “Privacy encompasses the right of a person to live his or her life as he or she pleases”; *NM v Smith* par [33]; Rautenbach “The Conduct and Interests Protected by the Right to Privacy” 2001 (1) *Journal of South African Law* (JSAL) 122.

⁴²⁷ *Bernstein v Bester* par [65-67]; *Estate Agency Affairs Board v Auction Alliance (Pty) Ltd* 2014 (4) BCLR 373 (CC) par [34].

⁴²⁸ *Ibid*; *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) v Smit* pars [17-18]; “The right [to privacy] is attenuated, not obliterated...” when a person moves into communal relations and activities” *Gartner v Minister of Finance* 2014 (1) BCLR 38 (CC) par [49].

⁴²⁹ *Minister of Constitutional Development v Prince* par [25-26]; Ss. 4(b) and 5(b) of Drugs and Drug Trafficking Act 140 of 1992; S.22A(9)(i) of the Medicines and Related Substances Control Act 101 of 1965; Schedule 7 of GN R509 of 2003.

⁴³⁰ *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1989 (1) SA 6 par [31] “[R]ights should not be construed absolutely or individualistically in ways which denied that all individuals are members of a broader community and are defined in significant ways by that membership...”.

⁴³¹ Ss. 4(b) and 5(b) of Drugs and Drug Trafficking Act 140 of 1992; S.22A(9)(i) of the Medicines and Related Substances Control Act 101 of 1965; Schedule 7 of GN R509 of 2003.

compared to public spheres.⁴³² The Court found that the right to privacy indicates the “right to a sphere of intimacy and autonomy that should be protected from invasion” especially from the State.⁴³³ Hence, the Constitutional Court held the prohibition of growing and smoking cannabis in a private home was unconstitutional.

3.5 The right to privacy of communications

Section 14(d) of the Constitution protects the privacy of communications from infringement. This suggests that persons communicating within a sphere of privacy are entitled to a reasonable expectation of the privacy of their communication.⁴³⁴ The Constitutional Court, in upholding the High Court’s decision in *AmaBhungane*, refers to communications surveillance as a “highly disturbing” invasion of privacy.⁴³⁵ The doctrine of reasonable expectation of privacy embodies an active participation by the persons engaging in communication to maintain such communication in the private realm.⁴³⁶ Once persons communicating shield their communications from the public realm, the constitutional protection of the right to privacy is invoked in a less attenuated manner.⁴³⁷ The constitutional protection of privacy is only triggered when there is an infringement on the general right to privacy.

The protection of the privacy of communication also affects other rights, such as the right to religion, belief and opinion and freedom of expression.⁴³⁸ One of the ways of enjoying these other rights is through communication. Information regarding religion, beliefs and opinion is referred to in the POPIA as special information. This indicates that the protection of the privacy of communication also affects information privacy. Hence, statutes regulating communications privacy must also not infringe unjustifiably the other rights also protected in the Bill of Rights.

⁴³² *Minister of Justice and Constitutional Development v Prince* par [43, 58, 66, 86].

⁴³³ *Minister of Justice and Constitutional Development v Prince* par [44]; *Bernstein v Bester* par [73]; *Case v Minister of Safety and Security*; *Curtis v Minister of Safety and Security* 1996 (1) SACR 587 (CC) par [91]; *Khumalo v Holomisa* par [27]; *Stanley v Georgia* 394 US 557 (1969) 559; *Ravin v State of Alaska* 437 P.2d 494 (1975); Brandeis J stated in, *Olmstead v United States* 277 US 438 (1928) 565, that privacy indicates “the right to be left alone”.

⁴³⁴ *Centre for Child Law v Media 24 Ltd* 2020 (1) SACR 469 pars [45-46]; *Financial Mail (Pty) Ltd v Sage* 462E-F; *Currie and De Waal The Bill of Rights Handbook* 295.

⁴³⁵ *AmaBhungane v Minister of Justice* (CC) par [24].

⁴³⁶ *Maharaj v Mandag Centre of Investigative Journalism NPC* 2018 (1) SACR 253 (SCA) par [34]; “It is basic to the principle of confidentiality that information cannot be protected once it loses its secrecy”; Loubser and Midgley(eds) *The Law of Delict in South Africa* 3ed (2018) 313, 391.

⁴³⁷ *AmaBhungane v Minister of Justice* (GP) par [29].

⁴³⁸ Rautenbach 2001 JSAL 117.

3.6 Limitation of rights in the Constitution

3.6.1 Overview of section 36 of the Constitution

The provisions of the Constitution reflect the will of the people, which signifies that the people have decided that these rights are worthy of protection.⁴³⁹ Consequently, the beneficiaries of the rights do not have to justify their enjoyment of the rights. Instead it is the State that must justify laws which limit such rights.⁴⁴⁰ Persons limiting the rights in the Bill of Rights must be accountable and “at the very least provide plausible [constitutionally valid] reasons for doing so”.⁴⁴¹ Any limitation that cannot be justified within the context of section 36 of the Constitution is invalid.

Section 36 of the Constitution is the general limitation clause and it sets out the criteria for justifying the restriction of the rights contained in the Bill of Rights.⁴⁴² Section 36 of the Constitution provides as follows:

- “(1)The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including –
- (a) the nature of the right;
 - (b) the importance of the purpose of the limitation;
 - (c) the nature and extent of the limitation
 - (d) the relation between the limitation and its purpose; and
 - (e) less restrictive means to achieve the purpose.
- (2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.”

The test for the constitutional validity of any limitation of a right and the factors mentioned in section 36(1)(a)-(e) are discussed below. Some rights in the Bill of Rights, for example the right to freedom of expression, have special limitation clauses and these rights are limited in terms of their special limitation clauses as well as the general limitation clause.⁴⁴³ The right to privacy does not have a special limitation

⁴³⁹ Rautenbach “Proportionality and the Limitation Clauses of the South African Bill of Rights” 2014 17 *Potchefstroom Electronic Law Journal (PELR)* 2234; Currie and De Waal *The Bill of Rights Handbook* 14.

⁴⁴⁰ *Ibid*; Currie and De Waal *The Bill of Rights Handbook* 8.

⁴⁴¹ *Teddy Bear Clinic for Abused Children v Minister of Justice and Constitutional Development* 2014 (1) SACR 327 (CC) par [84]; Rautenbach 2014 *PELR* 2232-2233.

⁴⁴² Rautenbach 2014 17 *PELR* 2248; Currie and De Waal *The Bill of Rights Handbook* 150.

⁴⁴³ S.16(2) of the Constitution.

clause and is limited by section 36 only.⁴⁴⁴ Before turning to the factors listed in section 36(1)(a)-(e) of the Constitution, the next section discusses the difficulty that arises in defining the terms “reasonable” and “justifiable” in section 36. It also establishes the rationale and benefits for the constitutional provision of guiding factors for defining the terms used. This jurisprudence is most useful for the development of the Nigerian law on the limitation of rights.

3.6.2 Reasonability and justifiability of limitations of rights

Section 36(1)(a)-(e) of the Constitution reflects the relevant considerations for the limitation of rights, which Chaskalson P in *S v Makwanyane* listed as requirements for determining the proportionality of a limitation.⁴⁴⁵ Although *S v Makwanyane* was decided under the Interim Constitution, the tests for justifying the limitation of rights in both Constitutions is similar.⁴⁴⁶ Section 33 of the Interim Constitution required that certain limitations be necessary in addition to being both reasonable and justifiable.⁴⁴⁷ Section 36(1) of the Constitution is more streamlined and does not require necessity as a test for justifying the limitation of the rights in the Bill of Rights.

Also, section 33 of the Interim Constitution did not provide a list of factors to be considered as in section 36(1)(a)-(e) of the Constitution. The current section 36 factors were developed in *Makwanyane* and were then incorporated into the Constitution as section 36(1)(a)-(e). These factors are not the test of constitutional validity, but are, according to Rautenbach, “instructions” and form part of the relevant considerations that are necessary in ascertaining whether the limitation of rights is reasonable and justifiable.⁴⁴⁸

The ultimate test for determining whether laws limiting the rights in the Bill of Rights are constitutionally valid is the reasonability and justifiability evaluation. Communications surveillance is a limitation of the right to privacy and raises the question of whether the communications surveillance regime in South Africa is

⁴⁴⁴ Rautenbach “The Limitation of Rights and “Reasonableness” in the Right to Just Administrative Action and the Rights to Access to Adequate Housing, Health Services and Social Security” 2005 4 *JSAL* 628.

⁴⁴⁵ 1995 (3) SA 391 par [104]; Rautenbach 2014 *PELR* 2240.

⁴⁴⁶ 200 of 1993.

⁴⁴⁷ S.33(b)(bb) of 200 of 1993.

⁴⁴⁸ Rautenbach 2005 4 *JSAL* 630.

reasonable and justifiable as mandated by section 36 of the Constitution.⁴⁴⁹ The South African jurisprudence is clear that the terms ‘reasonable’, ‘justifiable’ and ‘necessary’ cannot be interpreted appropriately in a vacuum and must be used by the courts for the purposes of “balancing”, “weighing” and/or determining the “proportionality” of limitation.⁴⁵⁰ The guidance provided by the factors in section 36(1)(a)-(e) of the Constitution ensures that courts are attentive to “matters that are essential” for the application of the general limitation test and that the courts avoid “instinctive and unmotivated conclusions and the development of abstract and rigid rules to apply the general test”.⁴⁵¹

The court also utilises the section 36 factors in adjudicating matters that have a common law element. This evaluation is usually not applied directly to the common law, but indirectly to align the underlying principles of common law with constitutional values and the Constitution itself. For instance, the Constitutional Court in *Barkhuizen v Napier* does not use the word justifiable.⁴⁵² However, the process of determining whether the time-limitation clause in issue in that case was fair and reasonable constituted a ‘reasonability and justifiability’ exercise in accordance with section 36(1)(a)-(e) of the Constitution.⁴⁵³

The factors of reasonableness and justifiability, phrased as “reasonably justifiable” in section 45(1) of the 1999 Constitution of Nigeria (the constitutional limitation clause), and as discussed in chapter 4 below, are utilised in limiting the right to privacy in Nigeria. However, the 1999 Constitution of Nigeria, unlike section 36 of the South African Constitution, lacks further guiding factors. As a result, the jurisprudence on section 45 of the Constitution of Nigeria is inconsistent, uncertain and sometimes conflicting. It needs reform and the South African jurisprudence is very valuable for this purpose, because it has benefitted from the guidance provided by the factors in section 36(1)(a)-(e). These factors are now discussed.

⁴⁴⁹ *AmaBhungane v Minister of Justice* (CC) par [25]; *AmaBhungane v Minister of Justice* (GP) par [41].

⁴⁵⁰ *Ibid*; *S v Bhulwana* 1996 (1) SA 388 (CC) par [18]; Currie and De Waal *The Bill of Rights Handbook* 162-163.

⁴⁵¹ Rautenbach 2005 JSAL 630.

⁴⁵² 2007 (5) SA 323 (CC) pars [47-60].

⁴⁵³ Currie and De Waal *The Bill of Rights Handbook* 62.

3.6.2.1 The nature of the right

When considering the nature of the right, courts examine the specific right in issue and the peculiar circumstances of each limitation. The evaluation of the nature of the right does not delineate some rights as being more important than others.⁴⁵⁴ Rather, it means that different aspects of a right are more important in certain instances.⁴⁵⁵ For example, while everyone is entitled to the right to privacy, the level of importance attached to a natural person is different to that of a juristic person. Also, the level of protection afforded to a person's activity in an inner sanctum is higher than that afforded in other spaces which fall outside of the inner sanctum.⁴⁵⁶ The consideration of the nature of the right therefore assists the court in determining the "kind of purpose that may justify the limitation and the scope."⁴⁵⁷

3.6.2.2 The importance of the purpose of the limitation

The purpose for which the limitation is sought must be identifiable and serve a "lawful purpose".⁴⁵⁸ The institution enforcing such a limitation must also have the authority to achieve the purpose of the limitation.⁴⁵⁹ The importance of the purpose of a limitation impacts significantly on the kind of limitation that a particular situation deserves.

Any statute limiting rights must state clearly the purpose of the limitation otherwise the statute will not meet the section 36(1)(b) requirement. With regard to communications surveillance and as discussed in section 3.8.2 below, the RICA authorises lawful interception of communications and acquisition of metadata in South Africa. There are also other statutes, such as the Criminal Procedure Act (CPA),⁴⁶⁰ the ECTA⁴⁶¹ and the Cybercrimes Act,⁴⁶² that refer to the RICA and that also have provisions on the utilisation of communications surveillance for various lawful purposes. These lawful

⁴⁵⁴ Rautenbach 2005 JSAL 631; Currie and De Waal *The Bill of Rights Handbook* 164.

⁴⁵⁵ *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In Re Hyundai Motor Distributors (Pty) Ltd v Smit* par [18]; *National Coalition of Gay and Lesbian Equality v Minister of Home Affairs* par [59]; *Phillips v Director of Public Prosecution* (WLD) 2003 (4) BCLR 357 (CC) par [23]; *Qwelane v South African Human Rights Commission* 2020 (2) SA 124 (SCA) par [51]; Rautenbach 2005 JSAL 631.

⁴⁵⁶ *Minister of Constitutional Development v Prince* pars [25-26].

⁴⁵⁷ Rautenbach 2005 JSAL 631.

⁴⁵⁸ *Minister of Welfare and Population Development v Fitzpatrick* 2000 (7) BCLR 713 (CC) par [20]; *National Coalition for Gay and Lesbian Equality v Minister of Home Affairs* 2000 (1) BCLR 39 (CC) par [59]; Currie and De Waal *The Bill of Rights Handbook* 164.

⁴⁵⁹ Rautenbach 2005 JSAL 631.

⁴⁶⁰ The Criminal Procedure Act 51 of 1977.

⁴⁶¹ The Electronic Communications and Transactions Act 25 of 2002.

⁴⁶² The Cybercrimes Act 19 of 2020.

purposes include activities of the State in securing criminal justice for serious crimes, the protection of lives, national safety and national security.⁴⁶³ These purposes, according to international law, are legitimate aims for communications surveillance, especially when considered on a case-by-case basis rather than as blanket aims.⁴⁶⁴

3.6.2.3 The nature and extent of the limitation

The nature and extent of the limitation are used to evaluate the limitation of the right and the extent to which the limitation affects the entrenched right. The court considers whether the limitation is proportionate to the benefits derived from the achievement of the purpose of the limitation.⁴⁶⁵ This consideration includes evaluating the identity of the persons authorised to execute the action that limits the right, and the extent of the powers the statute confers on them.⁴⁶⁶ The evaluation also assists the court in ensuring that the limitation does not infringe on the right more than is necessary.⁴⁶⁷

The consideration of the nature and extent of the limitation can also be identified in the international guidelines on interference with privacy, as discussed in chapter two.⁴⁶⁸ These guidelines indicate that communications surveillance may be utilised for serious crimes only.⁴⁶⁹ Any utilisation of communications surveillances for criminal activities, other than serious crimes, is considered overreaching and arbitrary.⁴⁷⁰ This is because the extent of intrusion of communications surveillance for less serious crimes is unreasonable, unjustifiable and unnecessary in a democratic society.⁴⁷¹

⁴⁶³ These legitimate aims are similar to those listed in article 8(2) of the ECHR; *Hulst v Netherland*, Communication No. U.N.Doc.CCPR/C/82/D/903/1999 par [7.7] (2004).

⁴⁶⁴ *Hulst v Netherland*, Communication No. U.N.Doc. CCPR/C/82/D/903/1999 par [7.7] (2004); UN Human Rights Committee (UN HRC), CCPR *General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* 8 April 1988 pars [4, 8].

⁴⁶⁵ *S v Bhulwana: S v Gwadiso* 1995 (12) BCLR 1579 (CC) par [18]; *Christian Education SA v Minister of Education* 2000 (10) BCLR 1051 (CC) par [51]; *S v Negal: S v Solberg* 1997 (10) BCLR 1348 (CC) par [168]; Rautenbach 2005 4 JSAL 632.

⁴⁶⁶ *Dawood v Minister of Home Affairs; Shalabi v Minister of Home Affairs; Thomas v Minister of Home Affairs* par [41].

⁴⁶⁷ Currie and De Waal *The Bill of Rights Handbook* 168.

⁴⁶⁸ Chapter 2, sec.2.2.2.5.

⁴⁶⁹ *Valenzuela Contreras v Spain* (1998) par [46]; *Malone* par [67]; *Huvig* par [29]; *Weber and Saravia* par [103-106]; *Bigbrother Watch v United Kingdom* App. Nos. 58170/13, 62322/14 and 24960/15, Judgment on 13 September, 2018 par [308]; *Kopp v Switzerland* (1998) par [64]; Annual Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, 39th session, Agenda items 2 and 3, A/HRC/39/27, 3 August 2018 par [38].

⁴⁷⁰ *Ibid.*

⁴⁷¹ Human Rights Commissioner's Annual Report on the Right to Privacy in the Digital Age, 27th session, Agenda 2 and 3, A/HRC/27/37, 30 June 2014, 21; Communication No. U.N.Doc. CCPR/C/50/D/488/1992 par [8.3] (1994).

3.6.2.4 The relation between the limitation and its purpose

Section 36(1)(d) of the Constitution considers whether the limitation is rationally capable of achieving the purpose of the limitation.⁴⁷² It also enquires into the extent to which the limitation can achieve the purpose without being too broad or too inclusive.⁴⁷³ It further considers whether the purpose of limitation in relation to its nature and extent is important enough to foster its justification in an open and democratic society based on human dignity, equality and freedom.⁴⁷⁴

3.6.2.5 Less restrictive means to achieve the purpose

Section 36(1)(e) of the Constitution refers to alternative means of achieving the purpose of the limitation.⁴⁷⁵ The availability of less restrictive means of achieving the purpose signifies that there are alternative means that “will either not restrict rights at all, or will not restrict them to the same extent” as the limitation under consideration.⁴⁷⁶ In order for less restrictive means of limiting a right to be preferred by the court, such means must be as effective as the limitation under consideration.⁴⁷⁷ The alternative means of achieving the purpose of limitation must also be proportional to the intended outcome, otherwise statutes authorising such limitation will be deemed overbroad.⁴⁷⁸ The procedure to be employed for the limitation of rights is a policy decision. Courts must be wary of second-guessing “the wisdom of policy choices made by legislators”.⁴⁷⁹

The factors considered above assist the court in the evaluation of constitutional validity and ultimately for the award of constitutional relief. The plaintiff may however pray for both constitutional relief and monetary damages. As discussed in section 3.7.3 below, the award of appropriate damages for infringement of privacy is usually assessed based on common law principles. The next section discusses the scope of the protection of the right to privacy in the South African common law and the assessment

⁴⁷² Rautenbach 2014 *PELR* 2232-2234; Andenas and Zleptnig “Proportionality: WTO Law: In Perspective” 2007 42 *Texas International Law Journal* 386.

⁴⁷³ *Case v Minister of Safety and Security*; *Curtis v Minister of Safety and Security* par [48-63]; *S v Manamela (Director-General of Justice Intervening)* 2000 (5) BCLR 491 (CC) par [96].

⁴⁷⁴ *Law Society of South Africa v Minister for Transport* 2011 (1) SA 400 (CC) par [47]; Rautenbach 2005 *JSAL* 634; Rautenbach 2014 *PELR* 2233; Cohen-Eliya and Porat *Proportionality and Constitutional Culture* (2013) 111-113.

⁴⁷⁵ Rautenbach *JSAL* 634.

⁴⁷⁶ Currie and De Waal *The Bill of Rights Handbook* 170.

⁴⁷⁷ *Ibid.*

⁴⁷⁸ Rautenbach 2005 *JSAL* 634; Currie and De Waal *The Bill of Rights Handbook* 171.

⁴⁷⁹ *Ibid.*; *S v Makwanyane* par [104]; Currie and De Waal *The Bill of Rights Handbook* 170.

of damages for infringement of privacy. Some valuable lessons are also drawn for Nigeria.

3.7 Invasion of privacy in terms of the South African common law

3.7.1 Overview of the common law protection of privacy

As mentioned earlier, the right to privacy is protected by the common law and classified as a personality right under the concept of *dignitas*.⁴⁸⁰ A claim for invasion of privacy resulting from a wrongful utilisation of communications surveillance may be appropriately compensated under the common law.⁴⁸¹ The interplay between the common law and constitutional relief for the infringement of rights with a dual protection under the common law and the Bill of Rights is discussed in section 3.7.4 below.

The remedy for the infringement of the right to protection of privacy at common law is the *actio iniuriarum*, which is an action for recovering compensation for non-patrimonial damage arising from wrongful and intentional infringement of personality rights.⁴⁸² The common law protects privacy as a personality right by prohibiting the unauthorised disclosure of private facts and the unlawful intrusion “upon the privacy of another”.⁴⁸³ Privacy is protected only to the extent to which a person causes the facts to be private and to the extent that any intrusion or disclosure is contrary to the legal convictions of the society.⁴⁸⁴

An individual who utilises communications surveillance wrongfully and intentionally could be liable in terms of the common law and also be guilty of an offence under the RICA.⁴⁸⁵ The wrongful utilisation of communications surveillance could result in

⁴⁸⁰ Neethling and Potgieter *Law of Delict* 421.

⁴⁸¹ *AmaBhungane v Minister of Justice* (CC) par [55].

⁴⁸² *O’Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) par [247]; *Gosschalk v Rossouw* 1966 (2) SA 476 (C) 490; Van der Walt and Midgley *Principles of Delict* 1; “Personality rights recognise a person as a physical and spiritual-moral being and guarantee his enjoyment of his own sense of existence.” Neethling, Potgieter and Roos *Neethling on Personality Rights* 3; Neethling and Potgieter *Law of Delict* 5.

⁴⁸³ *Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 (3) SA 56 (W) 60; Neethling *et al Personality Rights* 49; McQuoid-Mason *The Law of Privacy in South Africa* (1978) 37-39, 86-88; Neethling *et al Law of Delict* 422.

⁴⁸⁴ Neethling *et al Personality Rights* 46. Exceptions to determination of disclosure of private facts apply to persons who are incapable of authorising the disclosure, for example children, persons who are mentally disabled or unconscious persons who are mentally disabled or unconscious.

⁴⁸⁵ S.2 of 70 of 2002; S.49-51 of 70 of 2002 creates and punishes the offences of interception of communication and unlawful provision of real-time or archived communication-related information; *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 463; Van der Walt and Midgley

delictual liability on the basis of a wrongful invasion of privacy. The State could also be liable to compensate individuals for wrongful invasion of privacy. In the utilisation of communications surveillance, wrongfulness is the most important element for consideration as to whether liability arises.⁴⁸⁶ Other elements of delict such as conduct, causation, fault and damage are not usually in dispute in surveillance cases.⁴⁸⁷

3.7.2 Wrongfulness and communications surveillance

The common law element of wrongfulness is informed by the legal convictions of society, or *boni mores*. The legal convictions of society are, in turn, informed by the Constitution. Courts test common law principles against the Constitution to confirm their validity or develop them.⁴⁸⁸ This means that courts acknowledge external factors, such as Roman-Dutch and English laws which influenced the development of common law in South Africa, when adjudicating common law matters.⁴⁸⁹ The supremacy of the Constitution signifies a new constitutional era in which common law principles must be re-assessed in order to determine whether they need to be “replaced, supplemented or enriched” by constitutional norms.⁴⁹⁰ Wrongfulness consists of a duty not to infringe another person’s right without justification.⁴⁹¹

In the pre-constitutional era, wrongfulness was determined by the court’s interpretation of the legal convictions of society in each circumstance.⁴⁹² These convictions are not

Principles of Delict 3; Neethling *et al* *Personality Rights* 3; Neethling and Potgieter *Law of Delict* 424.

⁴⁸⁶ *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A) 462; *NM v Smith* par [34]; *National Media Ltd v Jooste* 270-272; *South African Broadcasting Corporation v Avusa Ltd* 2010 (1) SA 280 (GSJ) par [18]; *Tshabalala-Msimang v Mahkanya* 2008 (6) SA 102 (W) pars [45-50]; Van der Walt and Midgley *Principles of Delict* 171; Neethling and Potgieter *Law of Delict* 425.

⁴⁸⁷ *Ibid.*

⁴⁸⁸ *Steenkamp v Provincial Tender Board, Eastern Cape* 2007 (3) SA 121 (CC) par [41, 75]; *Country Cloud Trading CC v MEC Department of Infrastructure Development, Gauteng* 2015 (1) SA 1 (CC) par [21]; *Le Roux v Dey* 2011 (6) BCLR 577 (CC) pars [72-73]; *Carmichele v Minister of Safety and Security* 2001 (4) SA 938 (CC) par [56]; *Loureiro v iMvula Quality Protection (Pty) Ltd* par [53]. “The wrongfulness enquiry focuses on the conduct and goes to whether the policy and legal convictions of the community, constitutionally understood, regard it as acceptable. It is based on the duty not to cause harm-indeed to respect rights- and questions the reasonableness of imposing liability”; Van der Walt and Midgley *Principles of Delict* 6.

⁴⁸⁹ *Ibid.*; *De Klerk v Minister of Police* par [124, 138].

⁴⁹⁰ *Carmichele v Minister of Safety and Security* par [56].

⁴⁹¹ *De Klerk v Minister of Police* par [127]; *Loureiro v iMvula Quality Protection (Pty) Ltd* par [53]; *Country Cloud Trading CC v MEC, Department of Infrastructure Development, Gauteng* par [21].

⁴⁹² *Du Plessis v De Klerk* 1996 (3) SA 850 (CC) par [86]; Neethling and Potgieter *Law of Delict* 424; Van der Walt and Midgley *Principles of Delict* 33.

static.⁴⁹³ They also determine the boundaries of a permissible infringement of a right.⁴⁹⁴ The constitutional era changed the assessment of the legal convictions of society to an objective test based on the “spirit, purport and objects of the Bill of Rights”.⁴⁹⁵ Currently, the Bill of Rights is the norm upon which value judgments on policies and the legal convictions of the society are made. Hence, courts must discard “intuitive reaction to a collection of arbitrary factors”.⁴⁹⁶ However, the Bill of Rights does not exclusively reflect the legal convictions of society.⁴⁹⁷ Other factors considered in determining the legal convictions of society must align with constitutional values.⁴⁹⁸

Communications surveillance constitutes an infringement on privacy and is *prima facie* wrongful.⁴⁹⁹ The content of electronic communication and its metadata constitutes private facts of the parties of such communication.⁵⁰⁰ Thus, there is an objective expectation of privacy for the contents of communication and its metadata.⁵⁰¹ Communications surveillance can, however, be utilised for legitimate purposes, such as the preservation of rights and public interest.⁵⁰²

⁴⁹³ *H v Fetal Assessment Centre* 2015 (2) SA 193 (CC) par [67]; *Amod v Multilateral Motor Vehicle Accidents Fund (Commission for Gender Equality Intervening)* 1999 (4) SA 1319 (SCA) par [23]; Van der Walt and Midgley *Principles of Delict* 99.

⁴⁹⁴ The *boni mores* of the society or the current sense of justice of the society on the matter will be the determinant of the employer’s permissible limit in the circumstance. *Protea Technology v Wainer* 1997 (9) BCLR 1225 (W) 1241; Rycroft “Privacy in the Workplace” 2018 39 *Industrial Law Journal* 732; Modiba “Intercepting and Monitoring Employees’ E-mail Communications and Internet Access” 2003 *South African Mercantile Law Journal* 370.

⁴⁹⁵ *Country Cloud Trading CC v MEC Department of Infrastructure Development, Gauteng* 2015 (1) SA 1 (CC) par [21]; *Carmichele v Minister of Safety and Security* par [43, 54]; S.7(2) of the Constitution; *Minister of Safety and Security v Van Duivenboden* par [19-20]; *Loureiro v iMvula Quality Protection (Pty) Ltd* par [34].

⁴⁹⁶ *Telematrix (Pty) Ltd t/a Matrix Vehicle Tracking v Advertising Standards Authority* 2006 (1) SA 461 (SCA) par [16].

⁴⁹⁷ *Van Eeden v Minister of Safety and Security* 2003 (1) SA 389 (SCA) par [12]; Neethling and Potgieter *Law of Delict* 24; Van der Walt *Principles of Delict* 111.

⁴⁹⁸ *Ibid.*

⁴⁹⁹ *S v A* 1971 (2) SA 293 (T) 298; *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 463; *Sage Holdings Ltd v Financial Mail (Pty) Ltd* 1991 (2) SA 117 (W) 129, 130; *Motor Industry Fund Administrators (Pty) Ltd v Jamit* 1994 (3) SA 56 (W) 61; Rycroft “Privacy in the Workplace” 2018 39 *Industrial Law Journal* (ILJ) 725; Lawack-Davids “The Interception and Monitoring Bill-Is Big Brother Watching?” 2001 22 *Obiter* 347; Van der Walt and Midgley *Principles of Delict* 114; Neethling and Potgieter *Law of Delict* 424; Neethling *et al Personality Rights* 314.

⁵⁰⁰ Neethling *et al Personality Rights* 312-313. Neethling categorised intrusion into private facts as “(i) where such acquaintance is totally excluded or is limited to specific persons, and (ii) where the acquaintance is permissible to an indeterminate but limited number of persons”.

⁵⁰¹ Neethling *et al Personality Rights* 314; Neethling and Potgieter *Law of Delict* 421.

⁵⁰² *Tshabalala-Msimang v Mahkanya* par [45].

The inquiry into the wrongfulness of surveillance relates to whether the plaintiff should be compensated in light of the court's assessment of the legal convictions of society.⁵⁰³ "If wrongfulness has been established...a presumption of *animus iniuriandi* arises, which may be rebutted by the defendant".⁵⁰⁴ The legal convictions of society is not the society's moral, religious, social or ethical opinions on what is right or wrong.⁵⁰⁵ The inquiry into delictual wrongfulness is concerned with the allocation of legally recognised duties taking into account the "public and legal policy in accordance with constitutional norms".⁵⁰⁶

3.7.3 The Bill of Rights and the common law

The principles of common law that limit constitutional rights must align with the Constitution and must not unjustifiably infringe a right in the Bill of Rights or be contrary to the ethos of the Bill of Rights.⁵⁰⁷ The discussion in chapter two signifies that the availability of an effective remedy for abuse of communications surveillance by the State is one of the indicators of a regime that is lawful and non-arbitrary. The application of the values and norms of the Bill of Rights to the interpretation and development of ordinary laws (common law, statutes and customary law) is referred to as the indirect application of the Bill of Rights.⁵⁰⁸

The indirect application of the Bill of Rights requires that where the common law principles affect constitutional rights, public policy must be informed by constitutional

⁵⁰³ *De Klerk v Minister of Police* pars [124, 138]; *DE v RH* 2015 (5) SA 83 (CC) par [18]; *Mashongwa v Passenger Rail Agency South Africa* 2016 (3) SA 528 (CC) par [68]; *Telematrix v ASA* pars [12-13].

⁵⁰⁴ *NM v Smith* par [289]; See also *South African Broadcasting Corporation v Avusa Ltd* 2010 (1) SA 280 (GSJ) par [18]; *Tshabalala-Msimang v Mahkanya* par [45]; Neethling and Potgieter *Law of Delict* 425; Neethling *et al Personality Rights* 349.

⁵⁰⁵ *Du Plessis v De Klerk* 1996 (3) SA 850 (CC) par [86]; *Amod v Multilateral Motor Vehicle Accidents Fund (Commission for Gender Equality Intervening)* par [23].

⁵⁰⁶ *Lee v Minister for Correctional Services* 2013 (2) SA 144 (CC) par [55]; *Carmichele v Minister of Safety and Security* par [56]; *F v Minister of Safety and Security* 2012 (1) SA 536 (CC) par [119]; *Cape Town Municipality v Bakkerud* 2000 (3) SA 1049 (SCA) par [27]; *Gründling v Phumela Gaming and Leisure Ltd* 2005 (6) SA 502 (SCA) par [40]. The legal convictions of a society includes right thinking members of the society and those who practice in the industry where the action in dispute was undertaken. *Steenkamp v Provincial Tender Board, Eastern Cape* pars [40-43]; Van der Walt and Midgley *Principles of Delict* 100; Neethling and Potgieter *Law of Delict* 3.

⁵⁰⁷ *S v Manamela (Director-General of Justice Intervening)* par [32-33]; Neethling and Potgieter *Law of Delict* 18; Van der Walt and Midgley *Principles of Delict* 34.

⁵⁰⁸ S.39(2) of the Constitution; *Beadica v Trustees for the Time Being of the Oregon Trust* 2020 (9) BCLR 1098 (CC) par [71]; Currie and De Waal *The Bill of Rights Handbook* 31, 41- 42; South African Law Commission "Discussion Paper 109, Project 124 on Privacy and Data Protection" (October 2005) <https://www.justice.gov.za/salrc/dpapers/dp109.pdf> 5 (Chapter 2) (accessed 2019-04-10); Dafel *The Constitutional Rebuilding of the South African Private Law: A Choice Between Judicial and Legislative Law-Making* (2018) 63.

values.⁵⁰⁹ These constitutional values include the “notions of fairness, justice and reasonableness”.⁵¹⁰ Section 8(3) of the Constitution imposes a duty on courts to consider the interplay of principles of the common law between the private actors that led to the infringement of the right. The indirect application of the Bill of Rights in terms of section 8(3)(a) of the Constitution enables courts to look beyond the acts of the parties that limit the right, to the relevant principle(s) of the common law. The common law, customary law and several statutes pre-date the Constitution and they must be developed to conform to the “spirit, purport and objects of the Bill of Rights”.⁵¹¹

The Bill of Rights applies both vertically and horizontally. In terms of section 7(2) of the Constitution, the state, that is all spheres of government and organs of state, must respect, protect, promote and fulfil the rights in the Bill of Rights. Section 8(2) of the Constitution provides for the horizontal application of the Bill of Rights.⁵¹² The horizontal application of the Bill of Rights entails that a person whose privacy has been unlawfully infringed by, for example, the execution of communications surveillance by a private person, has recourse in terms of the common law, which will be interpreted through a constitutional prism.⁵¹³ The horizontality provision in the Bill of Rights has aided the courts in adjudicating matters where the actions of private individuals implicate the rights in the Bill of Rights.⁵¹⁴

The 1999 Nigerian Constitution, on the other hand, does not contain an express constitutional provision for the horizontal application of the Bill of Rights.⁵¹⁵ There is a mixed array of judicial decisions that are for, against and sometimes indifferent on the issue of horizontal application, as discussed in chapter four.⁵¹⁶ The issue is further complicated by an absence of a tort of privacy in Nigeria, with the Constitution being

⁵⁰⁹ *Barkhuizen v Napier* 2007 (5) SA 323 (CC) par [51]; *AB and CB v Pridwin Preparatory School* par [61].

⁵¹⁰ *Ibid*; *Beadica v Trustees for the Time Being of the Oregon Trust* par [71]; See also the preamble and s.1 of the Constitution.

⁵¹¹ “[T]he Bill of Rights...demand furtherance of its values mediated through the operation of ordinary law”; S.39(3) of the Constitution; *Barkhuizen v Napier* par [29]; *Carmichele v Minister of Safety and Security* par [56]; *Everfresh Market Virginia (Pty) Ltd v Shoprite Checkers (Pty) Ltd* 2012 (1) SA 256 (CC) par [48]; *NM v Smith* par [28]; Currie and De Waal *The Bill of Rights Handbook* 31.

⁵¹² Bilchitz “Privacy, Surveillance and the Duties of Corporations” 2016 *JSAL* 48.

⁵¹³ S.39(2) and (3) of the Constitution.

⁵¹⁴ *NM v Smith* pars [29-31].

⁵¹⁵ Nwauche “Securing Widows’ Sepulchral Rights through the Nigerian Constitution” 2010 23 *Harvard Human Rights Journal* 148.

⁵¹⁶ *Ibid*; *Mojekwu v Mojekwu* (1997) 7 NWLR 283 (C.A); *Muojekwu v Ejikeme* (2000) 5 NWLR 402, 436; *Onwo v Oko* (1996) 6 NWLR (Pt. 456) 584; *Uzoukwu v Ezeonu II* (1996) 6 NWLR (Pt.200) 708; Chapter 4; sec.4.4.1.

the only avenue for recourse of an infringement of privacy. Thus, an analysis of the positive effects of an express provision for horizontal application in the South African Constitution provides a basis to recommend changes for the development of a tort of privacy in Nigeria in order to create a better protection for the right to privacy. The common law and the 1999 Nigerian Constitution providing a dual protection for the right, is therefore a stronger route of protection.

3.7.4 The common law and constitutional relief

When discussing communications surveillance, the main focus is on the regulation of its use to curb arbitrary use by the State. Individuals whose communications are unlawfully surveilled suffer damage which ought to be compensated. Some rights entrenched in the Constitution, like the right to privacy, are also protected in terms of the common law, thereby providing dual protection for such rights.⁵¹⁷ This indicates that the South African jurisprudence on privacy combines the common law, the Constitution and legislation in providing protection for the privacy as recommended by international law.⁵¹⁸

The courts in South Africa usually award compensation in delict for the infringement of a right that is protected by both the law of delict and the Bill of Rights.⁵¹⁹ The flexibility of common law relief is such that it can accommodate a breach of constitutional rights if the court assesses it to be the most appropriate relief in the circumstances.⁵²⁰ Where the State unlawfully infringes the right to privacy, it may be liable both in terms of the law of delict and for an infringement of a constitutional right.⁵²¹ In a situation where the actions of the State are supported by statute, with regard to a right protected by the Constitution and common law, the applicant's remedy will be to request the courts to declare invalid the provisions of the law that do not align

⁵¹⁷ S.8(2) of the Constitution; *Khumalo v Holomisa* par [30-31, 33]; Currie and De Waal *The Bill of Rights Handbook*, 46.

⁵¹⁸ Article 17 of the ICCPR; Siracusa Principles par [A-8, B-18].

⁵¹⁹ *Mankayi v AngloGold Ashanti Ltd* 2011 (6) BLLR 527 (CC) par [17]; *NM v Smith* par [31]; *Law Society of South Africa v Minister for Transport* 2011 (2) BCLR 150 (CC) par [74]; *Fose v Minister of Safety and Security* 1997 (3) SA 786 (CC) par [60].

⁵²⁰ *Komape v Minister of Basic Education* par [41]; *Carmichele v Minister of Safety and Security* par [35-36]; *Fose v Minister of Safety and Security* par [58]; *Ngomane v Johannesburg (City)* 2020 (1) SA 52 (SCA) pars [22-27]; Van der Walt and Midgley *Principles of Delict* 7.

⁵²¹ S.39(3) of the Constitution provides that "[t]he Bill of Rights does not deny the existence of any other rights or freedoms that are recognised or conferred by common law, customary law or legislation, to the extent that they are consistent with the Bill."

with the Constitution.⁵²² Thereafter, the plaintiff can claim common law damages.⁵²³ Constitutional damages will only be awarded where common law relief is inadequate or inappropriate.⁵²⁴ Constitutional damages will as a general rule not be awarded if a delictual remedy is available.⁵²⁵ Nevertheless, the purpose of constitutional relief is not only to compensate the prejudiced party, but to affirm constitutional values.⁵²⁶

The purpose of the law of delict is to regulate relationships between private persons.⁵²⁷ It also serves to compensate an injured party for the wrong suffered, thereby providing for a wrong-doer to be held liable for his/her wrongful and culpable actions.⁵²⁸ The decision as to appropriate relief for an infringement of a right that has both delictual and constitutional elements must be decided in the light of the peculiarities of each case.⁵²⁹ A prejudiced party may claim delictual compensation against the State in addition to a declaration of rights and constitutional damages.⁵³⁰

Nigeria could also create an effective remedy for an infringement of the right to privacy which is unfortunately receiving little legal attention as discussed in chapter four.⁵³¹ Nigeria can also learn from South Africa's approach of combining the common law and the Constitution in adjudicating matters relating to infringements on the right to privacy. South Africa's jurisprudence on privacy has effectively combined the common law, the Constitution and legislation.

⁵²² *Komape v Minister of Basic Education* par [42]; *Minister of Police v Mboweni* 2014 (6) SA 256 (SCA) par [21].

⁵²³ *AmaBhungane v Minister of Justice* (GP) par [53, 68, 89]; *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg v Minister of Police* par [41].

⁵²⁴ *Fose v Minister of Safety and Security* par [60]. The Constitutional Court did not award constitutional damages in *Fose* but it provided some guidance on when constitutional damages will be appropriate. See too, *Thubakgale v Ekurhuleni Metropolitan Municipality* [2021] JOL 51813 (CC) par [47]; *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg v Minister of Police* par [97].

⁵²⁵ *Thubakgale v Ekurhuleni Metropolitan Municipality* par [83, 116]; *Steenkamp v Provincial Tender Board, Eastern Cape* par [29]; *Darson Construction (Pty) Ltd v City of Cape Town* 2007 (4) SA 488 (C) pars [509-510]; *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg v Minister of Police* par [97].

⁵²⁶ *Fose v Minister of Safety and Security* par [19]; See also *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg v Minister of Police* par [97]; *Thubakgale v Ekurhuleni Metropolitan Municipality* par [72]; Van der Walt and Midgley *Principles of Delict* 7.

⁵²⁷ *Fose v Minister of Safety and Security* par [17]; *NM v Smith* par [27].

⁵²⁸ Van der Walt and Midgley *Principles of Delict* 8.

⁵²⁹ *Komape v Minister of Basic Education* par [62]; *Hoffmann v SA Airways* 2001 (1) SA 1 (CC) par [55]; *Olitzki Property Holdings v State Tender Board* 2001 (3) SA 1247 (SCA) par [38]; *MEC, Department of Welfare v Kate* 2006 (4) SA 478 (SCA) par [25].

⁵³⁰ *Thubakgale v Ekurhuleni Metropolitan Municipality* [2021] JOL 51813 (CC) par [96]; Van der Walt and Midgley *Principles of Delict* 7.

⁵³¹ Nwauche "The Right to Privacy in Nigeria" 2007 1 *Centre for African Legal Studies Review of Nigerian Law and Practice* 64.

3.8 Statutory regulation of communications surveillance in South Africa

3.8.1 Overview of legislative regulation of communications surveillance in South Africa

The statutes that are considered in this section are specifically linked to the interception of communication and acquisition of metadata. These statutes are the POPIA, the RICA, the ECTA the Criminal Procedure Act (CPA) and the Cybercrimes Act. Communications surveillance is a multi-faceted programme involving different procedures before, during and after the surveillance.

As discussed in chapter one, communications surveillance is either targeted or untargeted (bulk). Targeted communications surveillance relates to an identified person and has two elements. These are the interception of the content of communications and the acquisition of metadata.⁵³² Metadata is the information relating to a communication and includes duration, length of call, location of transmission, names of recipients and sender, plus phone billing information.⁵³³ The surveillance of untargeted or bulk communications relates to the sifting of all communications within or outside the country of surveillance and usually concerns the communications of many unidentified persons.⁵³⁴

In South Africa, the RICA is the primary Act regulating communications surveillance.⁵³⁵ There are other statutes that regulate the activities of the State where communications

⁵³² Barbaro “Government Interference with the Right to Privacy: Is the Right to Privacy an Endangered Animal? 2017 6 *Canadian Journal of Human Rights* 128; Lordeain “EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era” 2015 3 *Media and Communication* 54; Newell “The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S and Europe” 2014 10 *Journal of Law and Policy* 487; Duncan *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (2018) 5; Vian “‘Veillant Panoptic Assemblage’: Mutual Watching and Resistance to Mass Surveillance After Snowden” 2015 3 *Media and Communications* 12.

⁵³³ *Ibid.*

⁵³⁴ *Centrum for Rattvisa v Sweden* (2019) 68 EHRR 2 par [7]; Samarajiva and Perera-Gomez “Bulk Data: Policy Implications (Draft)” (2018) <https://idi-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56922/56971.pdf> (accessed 2020-03-18); Bulk surveillance is also referred to as mass surveillance; United Nations General Assembly Report of the Special Rapporteur on the Right to Privacy, A/HRC/34/60, 34th session, 27 February - 24 March 2017, 11.

⁵³⁵ RICA does not provide for bulk surveillance; *AmaBhungane v Minister of Justice* (GP) par [165-166]; *AmaBhungane v Minister of Justice* (CC) par [24]; Duncan *Stopping the Spies* 98; Duncan *Stopping the Spies* 99; Kasrils “Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services” (10 September 2008) 8.4.2, the Ministerial Review Commission on Intelligence (Matthew’s Commission) confirmed the utilisation of bulk surveillance especially for the interception of foreign signals.

surveillance is necessary. For example, the POPIA protects personal information. As communications surveillance involves the processing of personal information, the POPIA, impacts communication surveillance indirectly.

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

3.8.2.1 Brief outline of the sections

The RICA is the main statute on communications surveillance in South Africa. This subsection explores the following aspects of the RICA: its objectives; its structure; and its problematic provisions. This approach allows the study to adopt a holistic approach.

3.8.2.2 Objective of the RICA

The RICA does not have a specific purpose clause, but its purpose is stated in its preamble.⁵³⁶ The primary objective of the RICA is to safeguard the right to privacy and other constitutional rights that may be affected by the surveillance of direct and indirect communication in South Africa. Direct communications are oral communications or utterances made while having an indirect communication in the presence of other persons.⁵³⁷ An indirect communication refers to transfer of information in any form through a postal service or telecommunications network.⁵³⁸ Indirect communications includes the content of communications and the metadata of an electronic communication.⁵³⁹

The RICA also regulates the following: the monitoring of radio frequency spectrums; the procedure for the application and granting of an interception of communication warrant; the granting of an entry warrant for the secret surveillance of a private property; and the kind of assistance a postal service provider or telecommunications network provider can render to a law enforcement agency. The RICA furthermore aims

⁵³⁶ Preamble of the RICA; *AmaBhungane v Minister of Justice* (GP) par [27]; Parliament of the Republic of South Africa “Annual Report of the Joint Standing Committee on Intelligence for the Financial Year Ending 31 March 2016” (13 December 2016)

<http://pmg-assets.s3-website-eu-west-1.amazonaws.com/intelligence.pdf> (accessed 2020-03-22) 28; Luck “Walking a Fine Line between Crime Prevention and Protection of Rights” 2014 538 *De Rebus* 1.

⁵³⁷ S.1 of 70 of 2002.

⁵³⁸ *Ibid.*

⁵³⁹ *Ibid.*; Metadata is referred to as communications-related information in the RICA.

to prohibit the operation of communications services networks that do not possess interception capabilities.⁵⁴⁰

The RICA further establishes the Office for Interception Centre (OIC) that is the head office of other interception centres.⁵⁴¹ These interception centres are the venues where the execution of communications surveillance will occur.⁵⁴² They maintain a connection to the CSPs network so that the surveillance subject's communications is sent to them for surveillance by LEAs.⁵⁴³ In other words, LEAs do not have direct access to CSPs networks, but the interception centres have a connection which is enabled to receive intercepted communications or conduct real-time surveillance when necessary.

The RICA does not specifically mention the protection of rights as its objective. This may imply that the aim of the RICA is focused more on combatting crimes rather than protecting rights. Duncan states that the RICA is one of the statutes enacted to combat the fight against global terrorism,⁵⁴⁴ while Bawa states that the enactment of the RICA was aimed at "equipping" LEOs in their fight against technologically sophisticated crimes.⁵⁴⁵ Duncan and Bawa's analysis rings true, especially considering the many loopholes in the RICA, as discussed below, that result in the infringement on rights unjustifiably. Although inadequate, chapter three of the RICA provides certain safeguards for the protection of the right to privacy. This indicates that the intention of the legislature was to ensure the protection of rights while also utilising communications surveillance.

Many of the provisions in the RICA also provide internal safeguards for privacy during the process of communications surveillance, for example, by limiting the number of persons that can legally access intercepted communication or communication-related information. Also, the RICA provides a sound structure that separates the different aspects of communications surveillance, even though it is utilised to provide lesser

⁵⁴⁰ S.30 of 70 of 2002.

⁵⁴¹ S.32-36 and 38 of 70 of 2002.

⁵⁴² S.32(1)(a) of 70 of 2002.

⁵⁴³ S.32(1)(c) of 70 of 2002.

⁵⁴⁴ Duncan *Stopping the Spies* 99.

⁵⁴⁵ Bawa "The Regulation of Interception of Communication and Provision of Communication-Related Information Act" <http://thornton.co.za/resources/telelaw13.pdf> (accessed 2020-03-30) 298.

protection to one aspect (metadata). Nevertheless, the RICA highlights the different categories and layers that are involved in targeted communications surveillance.

3.8.2.3 Selected terms in the RICA defined

The first chapter of the RICA defines the terms used in the Act. The RICA draws a distinction between direct and indirect communication. Direct communication is defined as an “oral communication, other than indirect communication, between two or more persons which occurs in the immediate presence of all persons participating in the communication”.⁵⁴⁶ An utterance by a participant of an indirect communication which is audible to persons physically present during the indirect communication is also referred to as direct communication.⁵⁴⁷

Indirect communication refers to the transfer of information either through postal services or telecommunications systems.⁵⁴⁸ Indirect communication is further classified into the content of communication and communication-related information. The content of communications is intercepted when it is acquired by a person who is not a participant of a direct or an indirect communication.⁵⁴⁹ The RICA utilises the term “intercept” for any surveillance of communications relating to the content only. This signifies that any interference with communication-related information (metadata) is not referred to as interception of communication.

Communication-related information is defined as any information that is generated from an indirect communication.⁵⁵⁰ Communication-related information is available with the telecommunications service provider and includes records of communication such as the time, duration, recipient, destination and termination.⁵⁵¹ It is also classified into real-time and archived communication-related information.⁵⁵² The former is communication-related information acquired within a 90 day period of the transmission

⁵⁴⁶ S.1 of 70 of 2002.

⁵⁴⁷ *Ibid.*

⁵⁴⁸ Indirect communications include telephone conversations, the contents of an e-mail transmission, facsimile, SMS, postal communication, and the downloading of information from the Internet. Bawa “The Regulation of Interception of Communication and Provision of Communication-Related Information Act” 298.

⁵⁴⁹ S.1 of the RICA defines intercept as “an aural or other acquisition of the contents of any communication... so as to make some or all of the contents available to a person other than the sender or recipient or intended recipient of that communication.”

⁵⁵⁰ S.1 of 70 of 2002.

⁵⁵¹ *Ibid.*

⁵⁵² S.1 of 70 of 2002.

of the indirect communication.⁵⁵³ The latter is any communication-related information acquired after 90 days from the day of transmission of the indirect communication.⁵⁵⁴ LEOs are required to apply for an interception or acquisition of real-time communication-related information direction before a designated judge.⁵⁵⁵ An interception or communication-related information direction is the judicial authorisation issued to a qualified LEO to execute targeted communications surveillance lawfully. An application for the acquisition of archived communication-related information is made before a judge of a High Court, a regional court magistrate or a magistrate.⁵⁵⁶ However, the interception of communication can only be ordered by a designated judge.

A designated judge is defined in section 1 of the RICA as:

“a judge of the High Court discharged from active service under section 3(2) of the Judges’ Remuneration and Conditions of Employment Act, 2001, or any retired judge, who is designated by the Minister to perform the functions of a designated for the purpose of this Act”

The qualification of the designated judge is specified in order to ensure that they are highly qualified and experienced.⁵⁵⁷ However, there are certain problems associated with the mode of appointment and the qualification of persons that can be appointed as a designated judge. This issue is discussed in subsection 3.8.2.5.1 below.

3.8.2.4 The structural and substantive framework of the RICA

The RICA regulates the lawful acquisition of the content of communications and its communication-related information.⁵⁵⁸ It also prohibits the unlawful interception of communication and the unlawful provision of communication-related information.⁵⁵⁹ It further provides for offences and penalties for unlawful execution of targeted communications surveillance.⁵⁶⁰

The RICA provides for a wide range of activities that are not directly related to the execution of targeted communications surveillance but aid the process. Some of these

⁵⁵³ *Ibid.*

⁵⁵⁴ *Ibid.*

⁵⁵⁵ S.16(1) and 17(1) of 70 of 2002.

⁵⁵⁶ S.19(1) of 70 of 2002.

⁵⁵⁷ *AmaBhungane v Minister of Justice* (GP) pars [32, 57, 60]; *AmaBhungane v Minister of Justice* (CC) par [76].

⁵⁵⁸ Ss.4 and 8 of 70 of 2002.

⁵⁵⁹ S.49 of 70 of 2002.

⁵⁶⁰ Ss.2-15 and 22 of 70 of 2002.

activities include the entry into a property for the purpose of connecting an interception device and decryption of electronic communications.⁵⁶¹ The RICA further includes provisions that relate to registration of cellular phone SIM-cards and the duties of telecommunications service providers and their customers.⁵⁶² It also prohibits the manufacturing of certain listed equipment.⁵⁶³

Chapter two distinguishes between the content of communication and communication-related information, dividing the two categories into part one and part two. It also provides that participants to communications can lawfully acquire the content of communication or its metadata.⁵⁶⁴ In addition, they can also authorise, in writing, other persons to acquire the content of communications and its communication-related information from their Telecommunications Service Providers (referred to here as communications service providers (CSPs)).⁵⁶⁵

Part one prohibits the unauthorised interception of communications, which, as explained earlier, relates to the content of the communication. It also specifies persons who may intercept communications. They are the postal service provider or a telecommunications service provider to whom an interception direction is addressed.⁵⁶⁶ LEOs are the only qualified applicants for an interception or communication-related direction.⁵⁶⁷ However, the actual process of interception or acquisition of communication-related information is a technical process and the expertise of the CSPs may be required.⁵⁶⁸

Telecommunications transmission automatically generates communication-related information. Only CSPs who are the licensed operators of the telecommunications service are permitted to store communication-related information.⁵⁶⁹ Provisions in the RICA relating to communication-related information are therefore mostly directed at CSPs. Business owners may also intercept indirect communications for business purposes, subject to the provisions of section 6 of the RICA. LEOs with the requisite

⁵⁶¹ Chapter 4 of 70 of 2002.

⁵⁶² Chapter 7 of 70 of 2002.

⁵⁶³ S.45 of 70 of 2002.

⁵⁶⁴ Ss.4 and 12 of 70 of 2002.

⁵⁶⁵ Ss.5 and 14 of 70 of 2002.

⁵⁶⁶ S.3(b) of 70 of 2002.

⁵⁶⁷ S.1 of 70 of 2002.

⁵⁶⁸ S.30 of 70 of 2002. The CSPs are not legally authorised to intercept communications that are transmitted through their networks

⁵⁶⁹ *Ibid.*

qualification may intercept communications without an interception direction in emergency situations.⁵⁷⁰ They must, however, submit a report of such activity to a designated judge as soon as practicable.⁵⁷¹

Chapter two, part two of the RICA, prohibits unlawful acquisition of communication-related information.⁵⁷² It also specifies the persons who are lawfully permitted or authorised to acquire communication-related information.⁵⁷³ The interception of communications and acquisition of communication-related information have mostly similar requirements with regard to lawfully authorised persons.

Section 15 of the RICA (which is in chapter two) provides that other statutes may also permit the lawful acquisition of communication-related information. Section 15(1) of the RICA provides that:

“Subject to subsection (2), the availability of the procedures in respect of the provision of real-time or archived communication-related information provided for in sections 17 and 19 does not preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any Act.”

Section 15 does not provide for procedures ensuring such statutes are on par with the RICA, unlike that of the interception of communications in section 9. The distinction between section 9 and 15 creates a hierarchy between contents of communication and communication-related information with the former having a higher status. Section 15 is discussed below in subsequent subsections. The impact of section 15 on section 205(1) of the CPA is also discussed in section 3.8.2.5.2 below.

Chapter three of the RICA sets out the procedure for applying for an interception and communication-related information direction. Chapter three also distinguishes the differences between the content of communication and communication-related information. The RICA further highlights the hierarchy created in section 15 by providing for a less stringent procedure for the application of communication-related information. Nonetheless, the same category of persons is authorised to apply for targeted communications surveillance directions.

⁵⁷⁰ Ss.5, 7 and 8 of 70 of 2002.

⁵⁷¹ S.8(4) of 70 of 2002.

⁵⁷² Ss.2 and 212 of 70 of 2002.

⁵⁷³ Ss.13 and 14 of 70 of 2002. As provided by s.1, the specified persons include members of the Police Service, Defence Force.

The RICA permits LEOs, with the authorisation of clearly defined and specified senior officers, to apply for an interception or communication-related direction.⁵⁷⁴ The specificity of the applicants in the RICA ensures that LEOs acquire content of communication and communication-related information in their areas of expertise only.⁵⁷⁵ The special categorisation of eligible applicants of surveillance directions has the potential of limiting applications for communications surveillance. Sections 42 and 43 of the RICA prohibit the disclosure of information acquired through surveillance, except to specified persons such as “any competent authority which requires it”.⁵⁷⁶ This provision further protects the information and limits unrestrained inter-departmental access to it. As discussed in chapters four and five, Nigeria can benefit from these provisions when protecting information acquired from communications surveillance.

Chapter three of the RICA continues with the hierarchy of protection between contents of communications and communication-related information. It provides a less stringent procedure for the acquisition of communication-related information compared to that of the content of communications.⁵⁷⁷ The differences in the procedure for applying for an interception and communication-related direction are discussed in detail in the next subsection. Chapter four of the RICA relates to procedure for physical entrance into

⁵⁷⁴ Ss.3, 4,5, 13,14 of 70 of 2002; *AmaBhungane v Minister of Justice* (GP) par [30]; *AmaBhungane v Minister of Justice* (CC) par [95]; S.1 of 70 of 2002 defines an applicant as:
“(a) an officer referred to in section 33 of the South African Police Service Act, if the officer concerned obtained in writing the approval in advance of another officer in the Police Service with at least the rank of the assistant-commissioner and who has been authorised in writing by the National Commissioner to grant such approval;
(b) an officer as defined in section 1 of the Defence Act, if the officer concerned obtained in writing the approval in advance of another officer in the Defence Force with at least the rank of major-general and who has been authorised in writing by the Chief of the Defence Force to grant such approval;
(c) a member as defined in section 1 of the Intelligence Services Act, if the member concerned obtained in writing the approval in advance of another member of the Agency or the Service, as the case may be, holding a post of at least general manager;
(d) the head of the Directorate or an Investigating Director authorised thereto in writing by the head of the Directorate;(e) a member of a component referred to in paragraph (e) of the definition of “law enforcement agency”, authorised thereto in writing by the National Director;
or (f) a member of the Independent Complaints Directorate, if the member concerned obtained in writing the approval in advance of the Executive Director”; Duncan *Stopping the Spies* 90.

⁵⁷⁵ *AmaBhungane v Minister of Justice* (GP) par [60].

⁵⁷⁶ S.42(1)(a) of 70 of 2002.

⁵⁷⁷ Ss.16, 17, 18 and 19 of 70 of 2002.

premises for the purpose of interception of communication.⁵⁷⁸ It also defines the procedure for decryption of messages.⁵⁷⁹

Chapter five of the RICA provides, *inter alia*, for the storage of information acquired from “targeted communications surveillance”.⁵⁸⁰ Chapter six makes provisions for the interception centres where telecommunications service providers can transfer specified communications for interception by the State.⁵⁸¹ Chapters five and six are important for this discussion because they provide for the storage of information acquired from targeted communications surveillance. Chapter seven provides for the duties between CSPs and their customers.

Chapter eight of the RICA prohibits persons who have lawfully acquired information in the execution of targeted communications surveillance from disclosure of that information. Section 42 provides a detailed list of persons who are lawfully authorised to receive such information for the performance of their duties. Chapter nine creates offences under the RICA. These offences include the unlawful interception of communications and unlawful acquisition of communication-related information.⁵⁸² They attract an imprisonment of ten years or fine of R2, 000, 000 for natural persons and R5, 000, 000 for juristic persons.⁵⁸³

3.8.2.5 The problematic provisions in the RICA

Even though the RICA contains many commendable provisions, there are a few problematic areas. When confirming the declaration of invalidity in *AmaBhungane*, the Constitutional Court added that the RICA is necessary for criminal justice procedure in the State, but does not adequately protect human rights.⁵⁸⁴ However, in both *AmaBhungane* cases the respective courts only dealt with those sections of the RICA that were disputed and canvassed before the High Court. There are a number of other problematic issues in the RICA, which also need to be considered. This section addresses all these problems, aiming to show that the loopholes in the RICA (and how some of these were addressed in *AmaBhungane*) provide valuable guidance for the development of Nigeria’s legal framework.

⁵⁷⁸ Ss. 26 – 28 of 70 of 2002.

⁵⁷⁹ S.29 of 70 of 2002.

⁵⁸⁰ S.30 of 70 of 2002.

⁵⁸¹ S.32 of 70 of 2002.

⁵⁸² Ss.49 and 50 of 70 of 2002.

⁵⁸³ S.51 of 70 of 2002.

⁵⁸⁴ *AmaBhungane v Minister of Justice* par (CC) pars [32 and 33].

This section consists of two parts. The first part considers the issues that the applicants in *AmaBhungane* raised and the High and Constitutional Courts' assessment thereof. The second part discusses the problems with the RICA not addressed in *AmaBhungane*.

3.8.2.5.1 The problems in the RICA as canvassed in *AmaBhungane v Minister of Justice*

(i) Overview of the applicants' arguments

The applicants argued that the RICA violates a number of rights including the rights to privacy, a fair hearing, access to court and a fair trial and freedom of expression.⁵⁸⁵ They challenged the constitutional validity of a number of the provisions in the RICA in the High Court, arguing that the contentious provisions failed to provide adequate safeguards for the right to privacy and other rights. These provisions are sections 1 (definition and appointment of the designated judge), 16 (application for a communications surveillance order), 35 and 37 (both sections provide for the processing of post-surveillance information) of the RICA.⁵⁸⁶ Two issues were not provided for in the RICA, namely post-surveillance notification of surveillance and the utilisation of bulk surveillance.

Whilst the applicants agreed that communications surveillance can serve "legitimate and important purposes" in a State,⁵⁸⁷ they contended that the limitation of these rights by RICA did not align with the requirements of section 36 of the Constitution and they thus sought a declaration of constitutional invalidity.⁵⁸⁸ The High Court upheld their claims and declared the contentious provisions in the RICA constitutionally invalid. This order was confirmed by the Constitutional Court.

⁵⁸⁵ Ss.16, 34 and 35 of the Constitution.

⁵⁸⁶ *AmaBhungane v Minister of Justice* (CC) pars [48, 94, 100, 108, 119, 135]. The contentions regarding ss. 1, 16, 35 and 37 was that they provided inadequate safeguards for communications surveillance.

⁵⁸⁷ *AmaBhungane v Minister of Justice* par [29].

⁵⁸⁸ The head of argument of the applicants in *AmaBhungane v Minister of Justice* https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf (accessed 2020-08-10) 4.

(ii) High Court and Constitutional Court Orders

The High Court upheld the applicant's claims and declared the contentious provisions in the RICA invalid. The High Court's declaration of unconstitutionality was upheld by the Constitutional Court to the extent that the RICA failed to:

- a) provide safeguards for a sufficiently independent designated judge;
- b) regulate post-surveillance notification;
- c) provide proper safeguards to address the impact of an *ex parte* interception direction application and order;
- d) prescribe proper procedures to manage the lawful use of intercepted communications; and provide proper protection where the subject of surveillance is a practising lawyer or journalist.

The declaration of unconstitutionality took effect from the date of judgment, namely 4 February 2021, and was suspended for 36 months to give Parliament an opportunity to amend the Act. During the period of suspension, the RICA was deemed to include the following additional sections:

"Section 23A Disclosure that the person in respect of whom a direction, extension of a direction or entry warrant is sought is a journalist or practising lawyer

- (1) Where the person in respect of whom a direction, extension of a direction or entry warrant is sought in terms of sections 16, 17, 18, 20, 21, 22 or 23, whichever is applicable, is a journalist or practising lawyer, the application must disclose to the designated Judge the fact that the intended subject of the direction, extension of a direction or entry warrant is a journalist or practising lawyer.
- (2) The designated Judge must grant the direction, extension of a direction or entry warrant referred to in subsection (1) only if satisfied that it is necessary to do so, notwithstanding the fact that the subject is a journalist or practising lawyer.
- (3) If the designated Judge issues the direction, extension of a direction or entry warrant, she or he may do so subject to such conditions as may be necessary, in the case of a journalist, to protect the confidentiality of her or his sources, or, in the case of a practising lawyer, to protect the legal professional privilege enjoyed by her or his clients.

Section 25A Post-surveillance notification

- (1) Within 90 days of the date of expiry of a direction or extension thereof issued in terms of sections 16, 17, 18, 20, 21 or 23, whichever is applicable, the applicant that obtained the direction or, if not available, any other law enforcement officer within the law enforcement agency concerned must notify in writing the person who was the subject of the direction and, within 15 days of doing so, certify in writing to the designated Judge, Judge of a High Court, Regional Court Magistrate or Magistrate that the person has been so notified.
- (2) If the notification referred to in subsection (1) cannot be given without jeopardising the purpose of the surveillance, the designated Judge,

Judge of a High Court, Regional Court Magistrate or Magistrate may, upon application by a law enforcement officer, direct that the giving of notification in that subsection be withheld for a period which shall not exceed 90 days at a time or two years in aggregate.”

The five specific issues canvassed by the applicants in *AmaBhungane* are now discussed.

(iii) Infringement on the right of access to court

Section 16(7)(a) of the RICA prohibits any disclosure to the subject of surveillance. The subjects of surveillance are not aware of the interference with their communications even after the investigation is concluded. As a result, they cannot “logically” approach the court for recourse if their right to privacy is infringed.⁵⁸⁹ This infringes the right of access to court as provided by section 34 of the Constitution.⁵⁹⁰

The applicants agreed that pre-surveillance notification defeats the purpose of the surveillance and is justifiable.⁵⁹¹ However, they contended that a prohibition of post-surveillance notification is contrary to section 36(1)(c) of the Constitution because it serves no justifiable purpose. They further contended that post-surveillance notification is the least restrictive means of limiting the right of access to court and that section 16(7)(a) of the RICA also does not align with section 36(1)(e) of the Constitution.

The respondent, on the other hand, argued that past surveillance cannot be erased and a post-surveillance notification is of no effect.⁵⁹² Sutherland J, upheld the applicant’s argument in part, reasoning that there may be cogent reasons, in extreme cases, for “perpetual secrecy” of communications surveillance.⁵⁹³ For this reason, he found that post-surveillance notification must be determined on a case-by-case basis.⁵⁹⁴ However, post-surveillance notification should be the “the default position” as

⁵⁸⁹ *AmaBhungane v Minister of Justice* (GP) par [43]; *AmaBhungane v Minister of Justice* (CC) pars [95-96].

⁵⁹⁰ S.34 of the Constitution provides that “[e]veryone has the right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum.”

⁵⁹¹ *AmaBhungane v Minister of Justice* (GP) par [41]; *AmaBhungane v Minister of Justice* (CC) par [95].

⁵⁹² *AmaBhungane v Minister of Justice* (GP) par [46].

⁵⁹³ *AmaBhungane v Minister of Justice* (GP) pars [44-45]; *AmaBhungane v Minister of Justice* (CC) par [48].

⁵⁹⁴ *AmaBhungane v Minister of Justice* (GP) par [54]; *Ibid.*

is the case in comparable democratic societies.⁵⁹⁵ This ruling was confirmed by the Constitutional Court, which added that post-surveillance notification serves two purposes.⁵⁹⁶ Firstly, post-surveillance notification enables the subject of surveillance to seek redress. Secondly, where the LEOs are aware that the surveillance subject can seek judicial review, this can “disincentivise” the arbitrary use of surveillance.

The discussion in chapter two detailed the African regional law guidelines on laws regulating communications surveillance. It indicated that post-surveillance notification is mandatory for Member States.⁵⁹⁷ At a global level, the HRC has adopted the reasoning of the ECtHR on surveillance matters.⁵⁹⁸ The decision of the High Court as confirmed by the Constitutional Court in *AmaBhungane* on post-surveillance notification is thus consistent with international and African regional law.⁵⁹⁹ It is also in line with section 233 of the Constitution that mandates courts to “prefer a reasonable interpretation of legislation that is consistent with international law”.

Furthermore, the Constitutional Court held that an automatic review may be implemented as surveillance subjects may be financially incapacitated to seek a review.⁶⁰⁰ An automatic review involves judicial evaluation of the surveillance procedure at no cost to the surveillance subject and assists to achieve redress in the event that rights have been infringed unlawfully. The Court further held that the automatic review should be a “summary” and “paper-based non-court procedure” with the designated judge reviewing the surveillance procedure.⁶⁰¹ This judge must be able to “call for whatever information she or he might require from whomsoever”.⁶⁰² This appears to include cross-examination of the LEOs, when necessary, to determine whether the surveillance procedure was lawfully executed and demonstrates that the designated judge acts as an inquisitor rather than an adjudicator.

⁵⁹⁵ *AmaBhungane v Minister of Justice* (GP) pars [47-51]; *AmaBhungane v Minister of Justice* (CC) par [48].

⁵⁹⁶ *AmaBhungane v Minister of Justice* (CC) par [45].

⁵⁹⁷ Principle 41 of the Declaration on Freedom of Expression and Access to Information, 2019 (2019 Declaration); Chapter 2, sec. 2.3.4.

⁵⁹⁸ 2014 OHCHR report; 2018 OHCHR report); 2014 OHCHR; The UN General Assembly resolution of the right to privacy in the digital age, 42nd session, A/HRC/42/L.18, 24 September 2019 (UN resolution on the right to privacy in the digital age).

⁵⁹⁹ 2014 OHCHR report, par [40]; Principle 41(3)(d) of the 2019 Declaration.

⁶⁰⁰ *AmaBhungane v Minister of Justice* (CC) par [50].

⁶⁰¹ *Ibid.*

⁶⁰² *Ibid.*

The automatic review procedure also strengthens the oversight function of judicial officers as the surveillance procedure will be subject to judicial review after its completion. The legislature, however, must determine the best course of action in terms of the principle of separation of powers.⁶⁰³ Nevertheless, the recommendation is an important one for the development of the law.

While the Court's recommendation for an automatic review may provide an effective and efficient avenue for redress, it does not provide a fair hearing to the surveillance subject if the designated judge reviews her or his own previous communications surveillance orders. That is, the designated judge should not review a communications surveillance order that she or he authorised, as this may result in bias. However, the designated judge can review the execution of the surveillance order and post-surveillance procedure that is implemented by LEOs.

The Court buttressed its recommendation for an automatic review with examples of this procedure in the South African legal framework as follows:

“automatic review by Judges of certain sentences imposed by magistrates and the automatic review of by the Land Claims Court of orders of eviction granted in the Magistrate's Courts”.⁶⁰⁴

These examples indicate that the review body is separate from the authorising body. Hence, the recommendation that the designated judge should perform an automatic review, does not align with the established practice where she or he is reviewing whether the grant of surveillance order was lawful. Nonetheless, a review mechanism is necessary to ensure that the surveillance process is thoroughly supervised. Automatic review is therefore recommended for Nigeria. Furthermore, there must be a different body to review the surveillance orders authorised by the designated judge. Ultimately, the court found that the RICA's provisions that prohibit notification to the surveillance subject infringe on the right of access to court and privacy. The right to privacy cannot be fully enjoyed if there is no recourse when infringement occurs. The right of access to court facilitates the seeking of recourse and is one of the indicators that a communications surveillance regime is lawful and non-arbitrary. Nigeria must

⁶⁰³ *AmaBhungane v Minister of Justice* (CC) par [54].

⁶⁰⁴ S.302 of the Criminal Procedure Act 51 of 1977; S.19(3) of the Extension of Security of Tenure Act 62 of 1997; *AmaBhungane v Minister of Justice* (CC) par [51].

avoid provisions that hamper the right of access to court by providing post-surveillance notification.

(iv) Infringement on the right to a fair hearing

The applicant's challenge to the RICA on the basis of a fair hearing was two pronged and based on the section 1 definition of designated judges, as well as section 16(7). The first challenge related to the independence and appointment of designated judges while the second challenge dealt with the absence of an adversarial process. These two challenges is discussed in the subsections below. They both relate to section 34 of the Constitution.

(a) The independence and appointment of designated judges

Section 1 of the RICA provides for the definition, mode of appointment, term of office and renewal of the term of designated judges. The Constitutional Court stated that section 1 of the RICA confers power on the Minister of Justice to appoint designated judges.⁶⁰⁵ Although, the power of appointment is not expressly conferred on the Minister of Justice by the RICA, it is enough that section 1 implies it through the definition of a designated judge.⁶⁰⁶

The applicants' contention with regard to independence of designated judges was two-fold. Both lines of argument were to the effect that the process of appointment, termination and term of office of a designated judge impedes their independence. The contention addressed the selection process of the designated judges, which was argued to lack the "requisite degree of independence".⁶⁰⁷ Firstly, the appointment, termination or renewal of term of a designated judge is at the "pleasure" of the Minister of Justice.⁶⁰⁸ Secondly, the RICA does not provide for the term of office of a designated judge.⁶⁰⁹ The respondents' defence was that it is the inherent duty of judges to be independent.⁶¹⁰ They also argued that some foreign jurisdictions, like Canada, UK and

⁶⁰⁵ *AmaBhungane v Minister of Justice* (CC) par [79].

⁶⁰⁶ *Ibid.*

⁶⁰⁷ *Glenister I* par [207].

⁶⁰⁸ *AmaBhungane v Minister of Justice* (GP) par [64]; *AmaBhungane v Minister of Justice* (CC) par [62, 79, 92].

⁶⁰⁹ *AmaBhungane v Minister of Justice* (CC) par [81].

⁶¹⁰ *AmaBhungane v Minister of Justice* (GP) par [63]; *AmaBhungane v Minister of Justice* (CC) par [89].

Australia appoint officials, who are not judges, to perform the role of the designated judge.⁶¹¹

The High Court, in upholding the applicant's argument, stated that the appointment of the designated judge is an impropriety to the institutional independence of the judiciary.⁶¹² Furthermore, the process of appointment, renewal and termination of the term of office of a designated judge must not, "induce, if only subliminally, an appetite to appease".⁶¹³ Section 1 of the RICA was, therefore, declared constitutionally invalid, because it failed to provide for an appointment mechanism of designated judges.⁶¹⁴ The Constitutional Court, in confirming the High Court's decision, held that the procedure of granting interception directions is not open to public scrutiny.⁶¹⁵ The RICA therefore does not provide for an accountability and oversight mechanism and lacks an adequate safeguard to ensure an independent judicial authorisation of interceptions.⁶¹⁶

The discussion in chapter two signifies that the independence of the oversight authority is a basic requirement of non-arbitrariness of a communications surveillance regime. The principle of accountability and separation of powers dictate that the oversight authority must be independent.⁶¹⁷ The HRC in its General Comment 16 stated that laws limiting privacy must "have clear provisions on the designated authority that is to permit such interference".⁶¹⁸

The ECtHR has also held that a judicial supervisory mechanism is the preferred option.⁶¹⁹ Nonetheless, Germany's utilisation of a non-judicial supervisory body was upheld to be adequate and effective.⁶²⁰ Germany's G 10 Act was transparent, provided

⁶¹¹ *Ibid.*

⁶¹² *AmaBhungane v Minister of Justice* (GP) par [63]; *AmaBhungane v Minister of Justice* (CC) par [89].

⁶¹³ *AmaBhungane v Minister of Justice* (GP) par [66]; *AmaBhungane v Minister of Justice* (CC) par [90]; *Helen Suzman Foundation v President of the Republic of South Africa*; *Glenister v President of the Republic of South Africa* 2014 (4) BCLR 481 (WCC) par [68] (*Glenister II*); *Justice Alliance of SA v President of Republic of South Africa* 2011 (10) BCLR (CC) par [73].

⁶¹⁴ *AmaBhungane v Minister of Justice* (GP) par [69]; *AmaBhungane v Minister of Justice* (CC) par [94].

⁶¹⁵ *AmaBhungane v Minister of Justice* (CC) par [93].

⁶¹⁶ *Ibid.*; *AmaBhungane v Minister of Justice* (CC) pars [93, 95].

⁶¹⁷ The Constitutional Court in *Amabungane* also emphasised the principle of separation of power as very important and it reflected when the designated judges are seen as independent in the eyes of a reasonable man. *AmaBhungane v Minister of Justice* (CC) par [87].

⁶¹⁸ General Comment 16 par [4].

⁶¹⁹ *Dumitru Popescu v Romania* (no. 2), App. No. 71525/01, (2007) par [71]; *Zahkarov v Russia* pars [233, 258].

⁶²⁰ *Weber and Saravia v Germany* par [115].

supervisory authority with full access to information and it was independent of the State.⁶²¹ Interestingly, the Russian regime presided over by judges was declared ineffective because it provided judges with limited access to information and this hampered their decisions.⁶²² An oversight mechanism must therefore be independent from the State and be well equipped to safeguard abuse of communications surveillance.⁶²³

Section 34 of the Constitution provides for the need to appoint an independent and impartial tribunal where appropriate. This indicates that the South African model of dispute resolution permits a non-judicial adjudicatory body where it is independent and impartial. The mere appointment of designated judges does not adequately reflect independence.⁶²⁴ The RICA's provision on an oversight mechanism on the communications surveillance is therefore an inadequate safeguard against arbitrariness. This aspect will be important to bear in mind for the reform of Nigeria's communications surveillance regulation.

(b) The procedure for an application for surveillance directions

The applicant's second point of contention on the issue of a fair hearing was that the application for surveillance is made *ex parte*, with section 16(7) of the RICA providing that the application of surveillance direction be made *ex parte*. This procedure negates the principle of *audi alteram partem*, which is important for a fair hearing.⁶²⁵ The applicants contended that the infringement of section 34 of the Constitution through section 16(7) was unjustifiable for various reasons. Firstly, they argued that there are less restrictive means of achieving the objectives of the RICA.⁶²⁶ They suggested the use of a public advocate as an alternative that does not abrogate a fair trial.⁶²⁷ The duty of the public advocate would be to represent the surveillance subject.

⁶²¹ *Dumitru Popescu v Romania* par [71]; *Zahkarov v Russia* pars [233, 258]; *Bigbrother Watch v UK* par [309].

⁶²² *Zahkarov v Russia* par [260].

⁶²³ *Ibid.*

⁶²⁴ *AmaBhungane v Minister of Justice* (CC) pars [89-91].

⁶²⁵ *AmaBhungane v Minister of Justice* (GP) par [72]; *AmaBhungane v Minister of Justice* (CC) par [96].

⁶²⁶ *Ibid.*

⁶²⁷ *AmaBhungane v Minister of Justice* (GP) par [76]; *AmaBhungane v Minister of Justice* (CC) par [99].

In response, the respondents contended that there is enormous security risk in the investigation of serious crimes.⁶²⁸ They argued that it is in the interest of national security to limit the persons involved in these investigations. They further contended that there is nothing that a public advocate will do that a diligent judge cannot do.⁶²⁹ Also, according to the respondents, there is “no room for testing evidence in these applications.”⁶³⁰ Some degree of faith has to be put in the applicants’ integrity not to mislead the judge with false evidence.⁶³¹

The High Court, in considering these arguments, disagreed with the notion that the principle of *audi alteram partem* is compatible with the concept of surveillance.⁶³² The High Court held that the right to a fair hearing must be differentiated from the condition for justification of surveillance.⁶³³ The Court furthermore reasoned that the applicant’s argument for justification of the infringement on the right to a fair hearing in this regard cannot rest on the principle of *audi alteram partem*.⁶³⁴ Rather, the argument is for a safeguard in the pre-surveillance phase that prevents the “unjust or unmeritorious authorisation of interception”.⁶³⁵ The High Court agreed that the provisions of section 16(7) of the RICA in which applications are made *ex parte* prevents the subject of surveillance from being heard.⁶³⁶ Section 16(7) of the RICA was therefore declared unconstitutional.⁶³⁷

The Constitutional Court aligned itself with the High Court on this issue.⁶³⁸ The Constitutional Court held that the problem is not that the application is made *ex parte*, as communications surveillance requires the subject of surveillance to be unaware of the surveillance.⁶³⁹ However, there are no mechanisms to ensure that there is a fair

⁶²⁸ *Ibid.*

⁶²⁹ *Ibid.*

⁶³⁰ *AmaBhungane v Minister of Justice* (GP) par [77]; *AmaBhungane v Minister of Justice* (CC) par [96].

⁶³¹ The applicant’s argument was based on s.36(e) of the Constitution.

⁶³² *AmaBhungane v Minister of Justice* (GP) par [74] “the condition upon which the secret spying process can be justified, i.e. fundamental values are reluctantly trampled on, with as light a thread as possible”; *AmaBhungane v Minister of Justice* (CC) par [97].

⁶³³ *Ibid.*

⁶³⁴ *Ibid.*

⁶³⁵ *Ibid.*

⁶³⁶ *AmaBhungane v Minister of Justice* (GP) par [82]; *AmaBhungane v Minister of Justice* (CC) par [99].

⁶³⁷ *Ibid.*

⁶³⁸ *AmaBhungane v Minister of Justice* (CC) par [100].

⁶³⁹ *AmaBhungane v Minister of Justice* (CC) par [96].

hearing as the information presented is one-sided in favour of the applicant.⁶⁴⁰ The judicial officer is then not in a position to verify or interrogate the information.⁶⁴¹

The High Court had suggested that a panel of designated judges, rather than one designated judge, may avert the risk of a “tunnel vision”.⁶⁴² The duty of the proposed public advocate in the application for a surveillance direction would be to present a diverse perspective that will assist the designated judge in the evaluation process.⁶⁴³ The High Court therefore agreed with the applicant’s argument albeit, using different reasoning, that is, recommending a panel of judges who can provide a diverse evaluation of the surveillance application. This indicates that there are less restrictive means available to overcome the problem of an interception application brought *ex parte*, currently provided for in the RICA. The Constitutional Court confirmed this position and held that parliament is in a better position to select the best option to provide safeguards for fundamental rights when applying for an interception direction.⁶⁴⁴

The second leg of the *audi alteram partem* argument related to the nature of the RICA proceedings. The purpose of chapter 3 of the RICA is to prevent the unmeritorious granting of surveillance directions. Sections 16(7)(a) provides that:

“[a]n application must be considered and an interception direction issued without any notice to the person or customer to whom the application applies without hearing such person or customer”.

Section 16(7)(a) prohibits notice to the subject of surveillance to be heard contrary to the requirements of an adversarial process. The RICA does not, in prohibiting the appearance of subjects of surveillance, prevent their case from being heard.⁶⁴⁵ Section 16(7)(b) provides that the designated judge can “require the applicant to furnish such further information as he or she deems necessary”. Judicial officers presiding over a surveillance direction application are not adjudicating an adversarial

⁶⁴⁰ *Ibid.*

⁶⁴¹ *Ibid.*

⁶⁴² *AmaBhungane v Minister of Justice* (GP) par [80].

⁶⁴³ *AmaBhungane v Minister of Justice* (GP) par [80].

⁶⁴⁴ *AmaBhungane v Minister of Justice* (CC) par [99].

⁶⁴⁵ *Independent Newspaper (Pty) Ltd v Minister for Intelligence Services: In Re Masetlha v President of the Republic of South Africa* par [45] “There may be instances where the interests of justice in a court hearing dictate that oral evidence of...confidential material related to police crime investigation methods or national security be heard in camera”.

process. Section 16(7)(b) places the presiding judge in an application for surveillance direction in an inquisitorial proceeding.

Although subjects of surveillance are not required to make physical representations, section 16(7)(b) ensures that their case is heard. The problem with section 16(7)(b) relates to whether the manner in which the case is heard permits a fair process. The principle of a fair hearing embodies the right to a procedure that allows fair considerations of both sides of the dispute.⁶⁴⁶ The Constitutional Court explained that a fair hearing in surveillance matters cannot be achieved where the presiding judicial officer is unable to verify the information provided by the applicant for an interception direction.⁶⁴⁷ The principle of *audi alteram partem* requires that the arbiter be informed of all points of views so as to evaluate the “cogency of any argument”.⁶⁴⁸ Hence, the rule of *audi alteram partem* is applicable to communications surveillance.

The Constitutional Court also held that the impunity of law enforcements officers regarding false information accompanying the application for interception direction is a factor that may aid the prevalence of falsifying evidence.⁶⁴⁹ It is therefore not enough that the information be provided by affidavit; the information provided to a judicial officer must be verified.⁶⁵⁰ The Constitutional Court’s proposed recommendation to overcome the problem of abuse of surveillance by LEOs is to reduce the secrecy surrounding the procedure by providing for post-surveillance notification to the subject of the surveillance.⁶⁵¹ This means that, in addition to the presiding judge being able to verify the information provided by the LEOs, the execution of the interception direction must be subject to post-surveillance transparency and accountability. Otherwise, there

⁶⁴⁶ *Twee Jonge Gezellen (Pty) Ltd v Land and Agriculture Development Bank of South Africa t/a the Land Bank* 2011 (3) SA 1 (CC) par [38].

⁶⁴⁷ *AmaBhungane v Minister of Justice* (CC) par [41].

⁶⁴⁸ *De Lange v Smuts NO* 1998 (3) SA 785 (CC) par [131]; *Bernstein v Bester* par [105]; *Stopforth Swanepoel & Brewis Inc. v Royal Anthem (Pty) Ltd* 2015 (2) SA 539 (CC) par [19]; *Cape Town City v South African National Roads Authority* 2015 (3) SA 386 (SCA) par [19]. “The logical corollary must therefore be that...the right to open justice must include the right to have access to papers and written arguments which are integral part of court proceedings.”

⁶⁴⁹ *AmaBhungane v Minister of Justice* (CC) par [41].

⁶⁵⁰ Justice Nkabinde confirms in her report that her office does a verification of the information presented in the affidavit for an application for an interception direction. The procedure for the verification is not stated but it indicates that the designated Judge has access to full information relating to the application. Annual report on interception of private communications to the Joint Standing Committee on Intelligence by Justice Nkabinde (17 March 2021) par [56].

⁶⁵¹ *AmaBhungane v Minister of Justice* (CC) pars [39,40].

will be rampant unlawful surveillance by LEOs that will be difficult to detect because of the secrecy of the post-surveillance procedure.⁶⁵²

The main problem that the Constitutional Court's recommendations addressed is the current practice of LEOs who sometimes act with impunity. The report of Justice Nkabinde, in her capacity as the designated judge, to the Joint Standing Committee on Intelligence (JSCI) also confirms that unlawful surveillance occurs.⁶⁵³ The RICA is therefore ineffective in curbing the excesses of LEOs if it does not ensure transparency and accountability post-surveillance.

Justice Nkabinde further stated in her report that law enforcement agencies by-pass the procedures in the RICA and conduct surveillance without an interception direction.⁶⁵⁴ It is recommended that in cases like this that both the LEO and the CSP should be held accountable. The RICA is clear that lawful communications surveillance is one that is authorised by a judge.⁶⁵⁵ The exception is in cases of emergencies where both the LEO and the CSP must report such cases to the designated judge. Also, interception of communications is to be executed by an interception centre. Consequently, a CSP that permits communications surveillance on its network in contravention of the RICA is an accomplice to the unlawful communications surveillance and should be punished accordingly.

The prosecution and investigation of some serious crimes, such as treasonable espionage, can be critical to the maintenance of national security.⁶⁵⁶ The High Court rightly stated that post-surveillance notification may be deferred for a longer term even posthumously if necessary.⁶⁵⁷ This indicates the sensitivity of some investigations and that fewer people need to be involved in the process in order not to jeopardise it.⁶⁵⁸

⁶⁵² *AmaBhungane v Minister of Justice* (CC) par [40]; Annual report on interception of private communications to the Joint Standing Committee on Intelligence by Justice Nkabinde (17 March 2021) pars [53,54,58].

⁶⁵³ Annual report on interception of private communications to the Joint Standing Committee on Intelligence by Justice Nkabinde (17 March 2021) par [58].

⁶⁵⁴ Annual report on interception of private communications to the Joint Standing Committee on Intelligence by Justice Nkabinde (17 March 2021) par [57].

⁶⁵⁵ S.3 of 70 of 2002.

⁶⁵⁶ *AmaBhungane v Minister of Justice* (GP) par [45]; *AmaBhungane v Minister of Justice* (CC) par [48].

⁶⁵⁷ *Ibid.*

⁶⁵⁸ *Independent Newspaper (Pty) Ltd v Minister for Intelligence Services: In Re Masetlha v President of the Republic of South Africa* par [45].

The inclusion of a public advocate, contrary to the High Court's decision, may therefore be more risky in some cases.

It has been shown, by way of the discussion of *AmaBhungane*, that the *ex parte* nature of the application does not prevent the subject of surveillance from being heard. The right to a fair hearing, unlike the right to a fair trial, does not require the presence of the subject of respondent; the mere presentation of the case suffices.⁶⁵⁹

In fact, an *ex parte* application for surveillance direction is the practice in comparable foreign jurisdictions. The ECtHR, in evaluating the surveillance regime of Germany and the UK, did not consider an *ex parte* application for surveillance directions as problematic.⁶⁶⁰ Russia's regime was, however, declared invalid.⁶⁶¹ Even though the Russian regime of surveillance is also *ex parte*, the presiding judges had limited access to information pertaining to the proceedings.⁶⁶² A well-informed oversight mechanism enables an appropriate consideration of the case of the subject of surveillance.⁶⁶³ The best practice for proper oversight mechanisms of communications surveillance direction requires independence, full access to information and a panel of at least three persons.

Other judicial officers, unlike designated judges, may be inexperienced or unfamiliar with the nature of communications surveillance legislation.⁶⁶⁴ An insufficient understanding of the intrusive nature of surveillance on privacy may lead to inadequate consideration of the matters relating to archived communication-related information. Hence, the independence of judges, regional magistrates and magistrates does not provide adequate safeguards for rights. This analysis has demonstrated that Nigeria needs a better process than that provided for in the RICA for its oversight mechanisms.

(v) Unlawful processing of post-surveillance information

The RICA provides for the storage of post-surveillance information for a minimum period of three months and a maximum period of five years. CSPs are mandated to ensure that their networks can store communication-related information and the State

⁶⁵⁹ *Twee Jonge Gezellen (Pty) Ltd v Land and Agriculture Development Bank of South Africa t/a the Land Bank* par [38].

⁶⁶⁰ *Bigbrother Watch v UK* par [303]; *Weber and Saravia v Germany* par [115].

⁶⁶¹ *Zakharov v Russia* pars [260-261].

⁶⁶² *Ibid.*

⁶⁶³ *Dumitru Popescu v Romania* par [71]; *Zakharov v Russia* pars [233, 258]; *Bigbrother Watch v UK* par [309].

⁶⁶⁴ *AmaBhungane v Minister of Justice (GP)* par [106].

can intercept it when necessary.⁶⁶⁵ They are also mandated to route duplicate signals to the Office of Interception Centres (OIC) were required by a surveillance direction.⁶⁶⁶

In *AmaBhungane*, the applicants' contentions concerning the processing of post-surveillance information was twofold. Firstly, they argued that the duration of the storage of post-surveillance information provided by the RICA is too long and therefore unreasonable.⁶⁶⁷ Secondly, the provisions of the RICA on the processing of the post-surveillance information are ineffective and have inadequate safeguards for privacy.⁶⁶⁸ The High Court disagreed with the applicant's assertion that a maximum of five years for the storage of information relating to electronic communications was too long in the South African context. Nonetheless, it upheld the applicant's argument on the inadequacy of the RICA in respect of the processing of post-surveillance information and declared sections 35 and 37 inconsistent with section 14 the Constitution.

It is clear that the storage of post-surveillance information serves a legitimate purpose. Comparable foreign jurisdictions attest to the necessity of storage of such information.⁶⁶⁹ A shorter duration for storage, however, is a less restrictive limitation to the right to privacy. The decision on the appropriate storage duration for post-surveillance information must be weighed and addressed in the context of the realities of each country, to be determined by a proportionality analysis. The analysis must consider the peculiar situation of the country in achieving the purpose of the limitation.⁶⁷⁰ Each country must therefore determine the adequate duration for storage of information in light of the context of their capabilities to achieve the purpose of the storage. The High Court, for example, considered the crime investigation capabilities in South Africa.⁶⁷¹ The conclusion was that a maximum period of five years is reasonable and in line with the "prescripts of section 36 of the Constitution".⁶⁷²

⁶⁶⁵ S.30(1)(a) and (b) of 70 of 2002.

⁶⁶⁶ S.30(3)(a)(iv) and (v) of 70 of 2002.

⁶⁶⁷ S.30(2)(a)(iii) of 70 of 2002.

⁶⁶⁸ *AmaBhungane v Minister of Justice* (GP) par [97]; *AmaBhungane v Minister of Justice* (CC) par [108].

⁶⁶⁹ QB in *R (Davis and Others) v Secretary of State for the Home Department* [2015] EWHC 2092 (17/07/2005) par [114].

⁶⁷⁰ Currie and De Waal *The Bill of Rights Handbook* 170-171.

⁶⁷¹ *AmaBhungane v Minister of Justice* (GP) par [95].

⁶⁷² *Ibid.*

Irrespective of the preferred duration of storage, there must be adequate safeguards for the processing of the information and the RICA is again deficient in this regard.⁶⁷³ Sections 35 and 37 of the RICA prescribe the powers, functions and duties of the Director of the Office for Interception Centres (Director). The duties include prescribing the information to be kept at the interception centres and ensuring that proper records are kept at the interception centres.⁶⁷⁴

The RICA does not prescribe the procedure for specific processing activities such as usage, transfer, erasure and copying. The respondents contended that the Minister of Communication's directives published in GN 1325 of 2005 (directives) prescribed the procedures for processing of post-surveillance information.⁶⁷⁵ The said directives provide a general prohibition of unauthorised dissemination of post-surveillance, but have no specific procedures for the processing of information by interception centres.⁶⁷⁶ The reality is that the processing of post-surveillance information forms an integral component of data privacy law and is protected in the POPIA. The accumulation of personal information can sometimes be as accurate as surveillance and can be useful in manipulating highly sensitive matters such as democratic elections.⁶⁷⁷ It may also be utilised to intimidate political opponents, adversely affecting democracy.⁶⁷⁸ It is therefore necessary that processing of such sensitive surveillance mechanisms be appropriately regulated, through a statute and not a subordinate directive.

The discussion in chapter two signifies that the HRC, with regard to communications surveillance, requires that the "legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive".⁶⁷⁹ This indicates that a Minister's directive is inadequate for prescribing the procedure to process post-surveillance information. The discussion in chapter two

⁶⁷³ 2011 Joint Standing Committee on Intelligence Report 26 par [16]. "The IG further noted that there was a lacuna/gap in the RICA Act (dealing with the handling of intercept materials)".

⁶⁷⁴ S.35 (e) and (f) of 70 of 2002.

⁶⁷⁵ *AmaBhungane v Minister of Justice* (GP) par [87]; *AmaBhungane v Minister of Justice* (CC) par [103].

⁶⁷⁶ *Ibid.*

⁶⁷⁷ Weber "The Digital Future-A Challenge for Privacy?" 2015 31 *Computer Law and Security Review* 238; Hirsch "The Law and Policy of Online Privacy: Regulation, self-regulation or co-regulation?" 2011 34 *Seattle University Law Review* 451.

⁶⁷⁸ *Ibid.*

⁶⁷⁹ Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 27th session, agenda items 2 and 3, A/HRC/27/37, 30 June 2014, par [29].

further indicates that legislation must provide specifically for the protection of data information as prescribed by data protection laws.⁶⁸⁰

The respondents in *AmaBhungane* argued that the POPIA provides procedures for processing of private facts and personal information that need not be duplicated by the RICA.⁶⁸¹ The applicants' contended that the POPIA does not eliminate the inadequacies in the RICA.⁶⁸² They further contended, which was accepted by the Constitutional Court, that a statute with adequate safeguards on processing of information should include:

“the procedure for examination, storage and use of data; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased.”⁶⁸³

The Constitutional Court, in confirming the decision of the High Court, stated that the provisions of sections 35(1)(f) and (g), and 42 of the RICA in respect of the processing of surveillance information were vague.⁶⁸⁴ The RICA only states that the OIC must retain particulars of the following: the application; the interception direction and the results obtained from execution of the interception direction.⁶⁸⁵ The RICA does not mandate the Director to store the application for interception, interception direction and the results obtained.⁶⁸⁶ The RICA does not, therefore, provide specific provisions to safeguard the processing of post-surveillance information.

The Constitutional Court held that the intercepted information is required for the subject of surveillance to make an informed decision on seeking redress.⁶⁸⁷ Furthermore, the decision on the manner in which the information obtained is to be

⁶⁸⁰ *Digital Rights Ireland* par [54]; *Liberty v United Kingdom*, App. No. 58243/001, (2008) par [62-63]; *Rotaru v Romania*, [GC], no.28341/95, (2000) par [57-59]; *S and Marper v United Kingdom*, [GC], App. Nos. 30562/04 and 30566/04, (2008) par [99]; *M.K. v France*, App. No. 19522/09, (2013), par [35].

⁶⁸¹ The heads of argument of the applicants in *AmaBhungane v Minister of Justice* https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf (accessed 2020-08-10) par [164].

⁶⁸² The heads of argument of the applicants in *AmaBhungane v Minister of Justice* https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf (accessed 2020-08-10) par [166].

⁶⁸³ The heads of argument of the applicants in *AmaBhungane v Minister of Justice* https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf (accessed 2020-08-10) par [151]; *Amabhungane v Minister of Justice* (CC) par [107].

⁶⁸⁴ *AmaBhungane v Minister of Justice* (CC) par [106].

⁶⁸⁵ *AmaBhungane v Minister of Justice* (CC) par [102].

⁶⁸⁶ *AmaBhungane v Minister of Justice* (CC) par [103].

⁶⁸⁷ *Ibid.*

processed is too vital to be left to the discretion of the Director.⁶⁸⁸ To this end, the Constitutional Court declared some sections of the RICA unconstitutional for failing to provide adequate safeguards that ensure that intercepted information is lawfully processed.⁶⁸⁹

The Constitutional Court did not, however, refer to the POPIA as a benchmark to which parliament can refer in amending the provisions of the RICA to rectify the invalidity. Perhaps the Constitutional Court was being careful not to overextend the issues due to the complexity of the relationship between the POPIA and the RICA, discussed in section 3.8.3 below, in terms of the exemption provided to the State in the former statute.

Post-surveillance information includes private facts and personal information. The POPIA gives effect to the right to privacy, provides for the protection of private facts and personal information,⁶⁹⁰ and regulates the processing of such facts and information.⁶⁹¹ The State, in executing communications surveillance, is involved in the processing of private facts and personal information. The POPIA, however, exempts the State from its provisions when investigating national security matters.⁶⁹²

The respondent's argument was partly correct because the POPIA can ameliorate the inadequacies in the RICA. Statutes must be read together and subsequent legislation constitutes "a 'legislative declaration' of the meaning parliament wishes to ascribe to earlier legislation".⁶⁹³ The POPIA was enacted over a decade after the RICA and parliament was more informed regarding technological advancement when the later statute was enacted.

However, as explained in section 3.8.3 below, the exemption of post-surveillance information involving national security matters is unqualified in the POPIA.⁶⁹⁴ As a result, personal information in a criminal investigation involving national security

⁶⁸⁸ *Ibid.*

⁶⁸⁹ *AmaBhungane v Minister of Justice* (CC) par [108].

⁶⁹⁰ S.2(a) of 4 of 2013.

⁶⁹¹ S.2(b) of 4 of 2013.

⁶⁹² S. 6 of 4 of 2013.

⁶⁹³ *Director of Public Prosecution, Western Cape v Prins* 2012 (2) SACR 183 (SCA) pars [37-38]; *National Education Health and Allied Workers Union v University of Cape Town* 2003 (3) SA 1 (CC) par [66]; *Sasol Synthetics Fuels (Pty) Ltd v Lambert* 2002 (2) SA 21 (SCA) par [15]; *Kent v South African Railways* 1946 AD 405.

⁶⁹⁴ S.6(c)(ii) of 4 of 2013.

matters is exempt from the POPIA.⁶⁹⁵ Although the POPIA complements the RICA, it does not eliminate entirely the unlawful processing of private facts and personal information by the State. Consequently, the processing of private facts and personal information in investigations involving national security matters is not protected by the RICA. The only recourse is in the common law for the protection of information that qualifies as private facts.

(vi) Infringement on the right to freedom of expression and fair trial

The applicants contended that the RICA provides inadequate safeguards for privileged communication involving confidential relationships, such as those involving legal practitioners and journalists.⁶⁹⁶ The applicants conceded that there are some safeguards in section 16(5) of the RICA, but the threshold is very low and does not provide expressly for the protection of these privileged relationships.⁶⁹⁷ They further argued that the right of journalists to freedom of expression (which includes freedom of the press and other media) is guaranteed in section 16(1) of the Constitution. The High Court agreed entirely with the applicants.⁶⁹⁸ Consequently, sections 16(5), 17(4), 19(4), 21(4)(a) and 22(4)(b) of the RICA were declared inconsistent with the Constitution. This is because the RICA provides inadequate safeguards for privileged relationships between attorney-client and journalist-sources. The protection of these relationships is a necessary instrument for a fair trial and freedom of the press as provided by section 35 and 16(1) of the Constitution respectively.⁶⁹⁹ The Constitutional Court also confirmed this decision in its entirety.⁷⁰⁰

(vii) Unlawful utilisation of untargeted (bulk) surveillance

The applicant's last contention was that untargeted surveillance in South Africa is unregulated and therefore unlawful. The respondents agreed that the RICA does not

⁶⁹⁵ *Ibid.*

⁶⁹⁶ *AmaBhungane v Minister of Justice* (GP) pars [110-113]; *AmaBhungane v Minister of Justice* (CC) par [112].

⁶⁹⁷ *AmaBhungane v Minister of Justice* (GP) pars [128-129].

⁶⁹⁸ *AmaBhungane v Minister of Justice* (CC) par [112].

⁶⁹⁹ *AmaBhungane v Minister of Justice* (GP) par [140]; *AmaBhungane v Minister of Justice* (CC) pars [115-117]. Other relationships such as those with laity and priests should also be considered. Furthermore, the COVID-19 pandemic has created a shift from physical to virtual meetings thus a number of legal matters are discussed virtually. Statutes must therefore have adequate safeguards to prevent confidential information from falling into the wrong hands.

⁷⁰⁰ *AmaBhungane v Minister of Justice* (CC) par [119].

provide for bulk surveillance,⁷⁰¹ but argued that the National Strategic Intelligence Act (NSIA) provides for bulk surveillance impliedly.⁷⁰² The High Court disagreed and declared that bulk surveillance in South Africa is unlawful.⁷⁰³ The Constitutional Court confirmed the High Court's declaration of unlawfulness of bulk surveillance.⁷⁰⁴

The NSIA specifically provides that the execution of interception and monitoring of communications must take place in terms of the RICA. Bulk surveillance is a form of monitoring of communication and is not regulated in the RICA.⁷⁰⁵ This indicates that the NSIA excludes its provisions from surveillance matters and instead refers to the RICA as the authorising statute in that regard. The NSIA therefore does not authorise surveillance of any kind. As mentioned earlier, Nigeria cannot derive lessons from a non-existent regulatory mechanism. However, the declaration of unlawfulness signifies that South Africa is mindful of her inadequacies in terms of regulating communications surveillance. The High Court held that a statute such as NSIA that does not provide expressly for bulk surveillance lacks clarity and is "at odds with the constitutional norm that guarantees privacy".⁷⁰⁶

3.8.2.5.2 Brief overview of additional problematic areas in the RICA

The problems with the RICA that are discussed in this sub-section were not raised in *AmaBhungane* and are analysed separately for ease of comprehension. One of the major problems with the RICA is the higher protection afforded to the content of communications as opposed to that of communication-related information, as is set out below. Ackerman J in *Bernstein v Bester* stated that "[a] very high level of protection is given to the individual's intimate personal sphere of life..."⁷⁰⁷ This signifies that the level of protection provided by the law over an activity determines whether it falls within the inner sanctum. The RICA therefore classifies the content of communication as falling within the inner sanctum, but does not similarly classify metadata. These issues are now discussed.

⁷⁰¹ *AmaBhungane v Minister of Justice* (GP) par [147]; *AmaBhungane v Minister of Justice* (CC) par [128].

⁷⁰² *Ibid*; S.2 of the National Strategic Intelligence Act 39 of 1994; *AmaBhungane v Minister of Justice* (GP) par [147, 153, 158].

⁷⁰³ *AmaBhungane v Minister of Justice* (GP) par [165]; *AmaBhungane v Minister of Justice* (GP) par [147]; *AmaBhungane v Minister of Justice* (CC) par [128].

⁷⁰⁴ *AmaBhungane v Minister of Justice* (CC) par [135].

⁷⁰⁵ *Centrum for Rattvisa v Sweden*, App. No. 35252/08 (2019) par [7].

⁷⁰⁶ *AmaBhungane v Minister of Justice* (GP) par [163].

⁷⁰⁷ *Bernstein v Bester* par [77].

(i) Lesser protection for communication-related information in other statutes

Chapter one of the RICA prohibits the unlawful interception of communications and unlawful provision of communication-related information. Most of these prohibitions are similar. However, section 9 of Part A provides that communications may be lawfully intercepted in prisons in terms of other statutes.⁷⁰⁸ Such statutes and regulations made in terms thereof must be submitted to parliament. However, the RICA does not state what the duty of parliament is with regard to the submitted statutes.⁷⁰⁹ It is assumed that parliament's duty is to scrutinise whether the statute or regulation contains provisions that conflict with the RICA. Nonetheless, it is clear from section 9 of the RICA that these other statutes may only provide for intercepting communications that are transmitted from prisons.

Section 15 of Part B of the RICA, on the other hand, provides that any other statute may provide for the acquisition of communication-related information. Section 15 does not have the same safeguards that apply to section 9. The only safeguard in section 15(2) is that such acquisition must not be on an on-going basis. The provisions of section 15 indicate that communication-related information is not considered as falling within the inner sanctum and thus does not qualify for the higher protection afforded to activities falling within the inner sanctum.

Communication does not fall within or outside the inner sanctum because of its kind or form, its time span, its transmission or storage. As discussed in section 5 of this chapter, the privacy of communications is constitutionally protected. Where a person engages in communication in the public realm, such communication is classified as falling within the inner sanctum and must be afforded a higher level of protection. Both real-time and archived communication-related information contain personal and private information relating to a person's communications and are protected by the right to privacy of communications.⁷¹⁰

By creating a hierarchy of communications between the content of communications and real-time communication-related information, on the one hand, and archived communication-related information, on the other, the RICA undermines the right to privacy and any violation would have to be justified in terms of section 36. During this

⁷⁰⁸ S.9(1) of 70 of 2002.

⁷⁰⁹ S.9(2)(a) of 70 of 2002.

⁷¹⁰ S.14(d) of the Constitution.

analysis an important factor that is discussed is that the current technology available for the acquisition of communication-related information renders an enormous volume of information accessible and is as intrusive as the content of communication.⁷¹¹ Classification of information acquired from communications surveillance should be utilised to aid the clarity of provisions in the statute and not for allocating higher protection to any information.

(ii) Lesser protection for archived communication-related information

The RICA gives the same weight and protection to any interference with the content of communications,⁷¹² that is, irrespective of whether interference with the content of communications occurs during or after the transmission of the communication.⁷¹³ However, the RICA subdivides communication-related information into real-time and archived communication-related information. The application for a real-time communication-related information direction must be made before a designated judge. Meanwhile, the application for an archived communication-related information direction has to be made before any other judicial officer.⁷¹⁴ That is, a judge of the High Court, regional magistrate or magistrate.⁷¹⁵

The designated judge must have the requisite expertise, experience and time.⁷¹⁶ Other judicial officers do not possess the same kind of specialised expertise of designated judges, but are tasked with the duty of considering an application for an archived

⁷¹¹ An analysis of metadata can reveal a person's movements at any given time, both virtual and physical contacts, time of contact, social circles, intimate relationships, routines, religious beliefs and interactions with protected sources or confidential clients; Crockford "Graphs by MIT Students Show the Enormously Intrusive Nature of Metadata" (7 January 2014) www.aclu.org/blog/national-security/secretcy/graphs-mit-students-show-enormously-intrusive-nature-metadata (accessed on 2020-01-30); Privacy International <https://privacyinternational.org/education/data-and-surveillance> (accessed on 2020-01-30); Report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014; Report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014; Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger* Judgment of 8 April 2014; *AmaBhungane v Minister of Justice* (GP) par [28], the High Court stated that RICA was enacted based on "what was understood to be the character of the telecommunications environment of that time"; Right to Know and Privacy International "The Right to Privacy in South Africa: Stakeholder Report Universal Periodic Review, 27th Session, South Africa" (October 2016) 5.

⁷¹² Ss. 1, 3, 16 of 70 of 2002.

⁷¹³ *Ibid.*

⁷¹⁴ S.19 of 70 of 2002.

⁷¹⁵ *Ibid.*

⁷¹⁶ *AmaBhungane v Minister of Justice* (GP) par [60].

communication-related information direction.⁷¹⁷ Furthermore, the fact that designated judges are retired signifies that they are not burdened with the daily expectations of regular court proceedings. This means that they should have time for the scrutiny of the application, which is necessary given the limitation to constitutional rights.

(iii) Difference in the requirements for application of intercept and communication-related direction

Section 16(2)(e) of the RICA provides that:

“If applicable, indicate whether other investigative procedures have been applied and have failed to produce the required evidence or must indicate the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence...”⁷¹⁸

This requirement enables the designated judge to determine whether there are other methods for acquiring the required information instead of intercepting communications. This provision has the potential of enabling LEOs to apply for an interception direction as a last resort since they have to convince the designated judge that there are no other viable options. This provision is absent in an application for communication-related direction.

(iv) Interception of communication where a law enforcement officer participates in the communication

The procedure for applying for an intercept direction, unlike the procedure for issuing a communication-related direction, provides more safeguards for preventing the arbitrary interception of communication. Section 4(2)(b) of the RICA enables LEOs to intercept communications if they are parties to the communication. In this situation, LEOs must satisfy themselves that they have fulfilled the requirements in section 16(5)(a), which provides for some of the grounds to be considered by a designated judge before issuing an interception direction.

There are two problems with the provisions of section 4(2)(b) of the RICA. Firstly, it is counterproductive for LEOs to evaluate whether they have complied with the provisions of RICA. This could lead to the arbitrary utilisation of information intercepted. Section 4(2)(b) undermines the designated judge, who is supposed to

⁷¹⁷ Duncan *Stopping the Spies* 92.

⁷¹⁸ S.16(2)(e) of 70 of 2002.

oversee the procedure for the purpose of transparency and accountability. As discussed in section 3.3.3 above, transparency and accountability are constitutional values that should be upheld, but this section of the RICA does not reflect accountability and thus does not align with the constitutional framework.

Secondly, there are other grounds in section 16(5)(b) and (c) that the designated judge must consider for determining whether to grant the intercept direction. These are, firstly, that a designated judge must be satisfied that there is a high possibility that the surveillance will yield positive results,⁷¹⁹ and secondly, that another investigative procedure has been applied and has failed to produce the required results.⁷²⁰ It is clear that the aim is to ensure that the oversight mechanism scrutinises the application to prevent inordinate applications for surveillance and ultimately to safeguard rights. However, section 4(2)(b) reduces the effect of such safeguards.

In spite of these problems in the RICA, there are many provisions that Nigeria can emulate, but with caution. The problematic areas above should be avoided to ensure good practice for the Nigerian context.

3.8.2.5.3 New issues in the RICA arising from the Constitutional Court's decision in *AmaBhungane v Minister of Justice*

While the Constitutional Court upheld the decision of the High Court, it also held that the RICA is silent on a number of other matters, thereby infringing privacy during surveillance, which limitation is egregiously intrusive.⁷²¹ The intrusion was held to be unjustifiable and arbitrary.⁷²² The Constitutional Court did not provide a new standard for determining whether there is adequate safeguard for fundamental rights during surveillance.⁷²³ Rather, there was an evaluation of the RICA to determine whether it is reasonable and justifiable in terms of section 36(1)(a)-(e) of the Constitution.⁷²⁴ This further buttresses the importance of a fixed guideline for determining whether laws are constitutionally valid and, as submitted in chapter four, is a good approach for Nigeria to emulate.

⁷¹⁹ S.16(5)(b) of 70 of 2002.

⁷²⁰ S.16(5)(c) of 70 of 2002.

⁷²¹ *AmaBhungane v Minister of Justice* (CC) pars [31, 35].

⁷²² *AmaBhungane v Minister of Justice* (CC) par [32]; *Minister of Safety and Security v Van der Merwe* 2011 (5) SA 61 (CC) pars [35-36].

⁷²³ *AmaBhungane v Minister of Justice* (CC) par [37].

⁷²⁴ *Ibid.*

(i) Absence of differentiation between intimate and non-intimate personal communications

Firstly, there is no differentiation in the RICA between intimate personal communications and communications that are not intimate.⁷²⁵ As discussed above, an inner sanctum is an exclusive intimate sphere that is determined by whether there is a reasonable expectation of privacy.⁷²⁶ A person has a reasonable expectation that communications sent through a CSP will not be interfered with by a third party.⁷²⁷

Communications surveillance intrudes into a sphere that is exclusively protected. The whole communication of the subject of surveillance, whether intimate or not, is already an exclusive intimate sphere. The differentiation that needs to take place is a consideration of what is relevant to the investigation or not. If intimate personal communications are relevant to the investigation, only then can they be assessed by a LEO.⁷²⁸

(ii) Lack of distinction between communications related or non-related to interception

Secondly, there is no differentiation in the RICA between communications relating to the interception and those that do not.⁷²⁹ An intrusion into communications that is not necessary for the investigation does not achieve any purpose. As a result, it is unreasonable to permit law enforcement officers to intrude into communications that are unnecessary for the investigation.⁷³⁰

Law enforcement officers are a party to an application for an interception direction, while the subject of surveillance is the other party. In order for both parties to be heard fairly according to section 35(3) of the Constitution, there must be a proportionate consideration of what information is required for the investigation. Practically, a law enforcement officer may not be able to determine precisely what evidence is required. However, in line with section 36(1)(d) of the Constitution, the party requesting a

⁷²⁵ *AmaBhungane v Minister of Justice* (CC) pars [24, 31].

⁷²⁶ *Bernstein v Bester* par [77]; *Prince v Minister of Justice* 2017 (4) SA 299 (WCC) pars [22]; *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC) pars [27-29]; *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) v Smit* pars [17-18].

⁷²⁷ S.14(d) of the Constitution.

⁷²⁸ *Bernstein v Bester* par [67].

⁷²⁹ *AmaBhungane v Minister of Justice* (CC) pars [24, 31].

⁷³⁰ S.36(1)(d) of the Constitution.

limitation of rights, usually the State, must prove that the limitation can achieve the purpose for which it is required. This indicates that LEOs should at the very least have an idea of the nature of the evidence they are searching for in the communications of the potential subject of surveillance. A third party is needed to mitigate against the intrusion that may occur by separating communications that are not relevant to the evidence. This consideration ensures that the limitation is not too broad for the intended purpose.⁷³¹ In this regard, the applicant in *AmaBhungane* argued in the High Court that a public advocate should be appointed to sieve through the communications.⁷³² It is thus recommended that when amending the RICA, the legislature should consider appointing a third party who must be capable of handling even the most delicate investigations.

(iii) Lack of protection of the fundamental rights of collateral victims

The Constitutional Court pointed out that the RICA did not state how the communications of persons who are not the subjects of surveillance are to be protected.⁷³³ The Constitutional Court refers to persons whose privacy may also be violated by surveillance and interception as collateral victims.⁷³⁴ This is because persons who respond to a communication have a reasonable expectation of privacy that there will be no third party intruding on their replies. Consequently, collateral victims are automatically deprived of their constitutional rights simply because they have communicated with the subject of surveillance.

Collateral victims of communications surveillance are also deprived of their right of access to court. Similar to subjects of surveillance, collateral victims are not provided with post-surveillance notification even though their communication with the latter was intercepted. The protection of the rights of collateral victims is further complicated by an inadequate awareness of the infringement of their rights during surveillance. While there is a global concentration on the protection of the rights of subjects of surveillance, the protection of the rights of collateral victims is neglected. The Constitutional Court's consideration of the protection of collateral victims is, therefore, commendable. Since

⁷³¹ *Law Society of South Africa v Minister for Transport* par [47]; Rautenbach 2005 JSAL 634; Rautenbach 2014 PELR 2233; Cohen-Eliya and Porat *Proportionality and Constitutional Culture* (2013) 111-113.

⁷³² *AmaBhungane v Minister of Justice* (CC) par [31].

⁷³³ *Ibid.*

⁷³⁴ *Ibid.*

there is no specific order by the Constitutional Court regarding collateral victims, it can only be hoped that parliament will consider their protection thoroughly when the RICA is amended.

There are two further infringements of rights, other than the right to privacy, that affect the rights of collateral victims. These are the right of access to court and the right to a fair hearing in terms of sections 34 and 35(3) of the Constitution respectively. In respect of the right of access to court, collateral victims are entitled to post-surveillance notification, just like the subjects of surveillance. This will enable them to achieve redress for any unlawful infringements on their rights. However, post-surveillance notification may be unnecessary if their part of the communication with the subject of surveillance is deleted before the execution of the interception direction.

Secondly, the collateral victims' right to a fair hearing is also infringed during interception of communications. This is because the interception direction is directed to the subject of the surveillance. Hence, collateral victims do not have an opportunity for a judicial officer to consider whether their communications with the subject of surveillance are necessary for surveillance and the manner of protection that should be accorded to them during interceptions. The fundamental rights of collateral victims of surveillance are therefore currently unreasonably and unjustifiably infringed in South Africa.

(iv) Special protection for certain categories of persons during communications surveillance

The Constitutional Court in *AmaBhungane* upheld the High Court's decision to the effect that the communications of lawyers and journalists must be given special consideration during surveillance.⁷³⁵ Lawyers and journalists have a duty of confidence to their clients and informants respectively and their communications need to be confidential.⁷³⁶ The Constitutional Court expounded further on the need to identify people who may fall into a special category of vulnerable groups and who may have certain specific fundamental rights accorded to them. For example, clients of legal practitioners may be deprived of their professional privilege, which affects their

⁷³⁵ *AmaBhungane v Minister of Justice* (CC) par [119].

⁷³⁶ Ss.34 and 35(3) of the Constitution; *Thint (Pty) Ltd v National Director of Public Prosecutions*; *Zuma v National Director of Public Prosecutions* 2008 (12) BCLR 1197 (CC) par [83].

rights to a fair hearing and a fair trial.⁷³⁷ Freedom of expression is very important for effective journalism and it is in the public interest to ensure the protection of this right for the preservation of democracy.⁷³⁸ Consequently, the Constitutional Court agreed that special protection should be afforded to them during surveillance.

Surveillance diminishes the preservation of confidentiality in communications and may deprive subjects of surveillance or collateral victims of the legal protection needed for the confidentiality of their communications. The persons who can be placed in this special category are not limited to those mentioned in the *AmaBhungane* case. For example, medical officers such as doctors and nurses who are likely to possess sensitive information about their patients, may also be included. Judicial officers should therefore be notified of people at risk.

These special categories of people also include children.⁷³⁹ The Constitutional Court declared that children should also be afforded special consideration because they are entitled to have their best interests regarded as paramount in every matter.⁷⁴⁰ The protection of the best interest of a child is also a fundamental right recognised by section 28(2) of the Constitution and article 3(1) of the Convention on the Rights of the Child.

The arguments for protection of special category of persons and the complexity of such groups in surveillance must always be evaluated by the judicial official presiding over a surveillance application. For example, even though children have a right to privacy like everyone else, they also have a fundamental right to have their best interest regarded as paramount in decisions relating to them. For their best interest to be considered, their age must be specifically mentioned to the judicial officer.

It is, therefore, important that communications surveillance applications be considered on a case-by-case basis and that presiding judicial officers have access to all

⁷³⁷ *AmaBhungane v Minister of Justice* (CC) pars [112,116-119].

⁷³⁸ S.16 of the Constitution; S.9 of the Children's Act 38 of 2005; Article 16(1) of the Convention on the Rights of Child; Article 10 of the African Charter on the Rights and Welfare of the Child; *Khumalo v Holomisa* par [24].

⁷³⁹ *AmaBhungane v Minister of Justice* (CC) par [115].

⁷⁴⁰ *Director of Public Prosecutor, Transvaal v Minister of Justice and Constitutional Development* 2009 (7) BCLR 637 (CC) pars [72-73]; *Centre for Child Law v Media 24 Limited* par [37]; S.28 (1)(g) of the Constitution provided special protection to the children to the effect that may only be detained for the shortest period and also provided a separate space from adults during the detention. This indicates that children must be provided with special consideration which is in their best interest in all instances that pertains to them.

information relating to the subject of surveillance.⁷⁴¹ This will enable the presiding judicial officer to provide the necessary protection to the person in question based on their unique situation. This is one of the reasons why a presiding judge(s) in a surveillance application must act as an inquisitorial panel.⁷⁴²

It is clear that the RICA has neglected to address adequately many issues that negatively impact fundamental rights. The Constitutional Court thus declared the RICA constitutionally invalid to the extent that it fails to provide adequate safeguards for the right to privacy, right to a fair trial and a fair hearing. The declaration of invalidity is suspended for a period of three years. It is expected, as argued by the respondents, that parliament will amend the law within this time period.⁷⁴³ Parliament must, therefore, be fully informed about the nature of communications surveillance and its effect on fundamental rights. A particular focus should be placed on an understanding of the complexities of the digital age in order to provide protection that can match rapid changes in technology.

The next section discusses the 2021 annual report of the designated judge submitted after the Constitutional Court's judgment in *AmaBhungane*. The discussion evaluates whether the interim orders in *AmaBhungane* are being practically implemented so as to make recommendations for Nigeria.

3.8.2.6 Report of the Designated Judge on the authorisation of interception directions

In line with the provisions of section 3(a)(iii) of the Intelligence Services Oversight Act,⁷⁴⁴ the designated judge is required to provide an annual report to parliament on the status of interception orders and compliance with the RICA in this regard.⁷⁴⁵ Justice Nkabinde's 2021 report as the designated judge provided an overview of the

⁷⁴¹ 1988 UN Human Rights Committee CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence and Protection of Honour and Reputation par [4].

⁷⁴² Defendants in a normal trial are represented by a legal practitioner who will present all facts that are necessary for a favourable outcome. Defendants in surveillance case should also have the same opportunity in the form of judges being presented with all information relevant to the case and not just those that the applicant consider as favourable for his/her case.

⁷⁴³ *AmaBhungane v Minister of Justice* (CC) pars [139-140].

⁷⁴⁴ 40 of 1994.

⁷⁴⁵ Justice Nkabinde's 2021 report par [1]. This report is for the period covering 1 November 2018 to 28 February 2021.

legal framework on communications surveillance in South Africa and the High and Constitutional Court's decisions in *AmaBhungane*.⁷⁴⁶

The designated judge stated that the process of an application for an interception direction to her office includes a confirmatory sworn affidavit from the OIC.⁷⁴⁷ The designated judge also stated that her office verifies the accuracy of cellular phone numbers that are submitted for interception.⁷⁴⁸ In her opinion, verification will ensure that fraudulent applications for interception of communications are not authorised.⁷⁴⁹

This report raises two issues for consideration. First, the details of the verification conducted by the OIC seems to relate to the issue of technical deficiencies.⁷⁵⁰ As a result, there is still no means of verifying the truth of the supporting information provided by LEOs to the designated judge to justify their application for an interception direction. Secondly, even though the report acknowledged the judgment of the Constitutional Court regarding the unconstitutional provisions in the RICA, there was no statement regarding how the Court's judgment will be applied to the future authorisation of interception orders. One would have expected that the report would state, for example, that future interception directions will provide for a post-surveillance notification. There is, therefore, no implementation strategy for Nigeria to observe from this report.

To sum up the discussion on the RICA, without the Constitutional Court's interim relief in *AmaBhungane* and the incorporation of the Court's recommendations, the execution of communications surveillance would be unlawful and arbitrary in South Africa. It is necessary for parliament to amend the RICA. Otherwise, the right to privacy and the rights to a fair hearing and fair trial will continually be unjustifiably infringed when executing communications surveillance.

3.8.3 The Protection of Personal Information Act, 2013

The POPIA gives effect to the right to privacy in section 14 of the Constitution by protecting personal information from unauthorised and/or unregulated processing and

⁷⁴⁶ Justice Nkabinde's 2021 report pars [8-32].

⁷⁴⁷ Justice Nkabinde's 2021 report par [52].

⁷⁴⁸ Justice Nkabinde's 2021 report par [56].

⁷⁴⁹ *Ibid.*

⁷⁵⁰ Justice Nkabinde's 2021 report par [52].

disclosure.⁷⁵¹ The POPIA regulates the processing of personal information by public and private bodies.⁷⁵² It establishes minimum requirements for the lawful processing of personal information and responsible parties are mandated to adhere to these.⁷⁵³ The POPIA is currently in operation and responsible parties have to be fully compliant with the provisions of the POPIA.

The interpretation of the POPIA is contingent upon understanding the key terms defined in section 1 of the Act.⁷⁵⁴ Some of the terms relevant to communications surveillance include “personal information”, “electronic communication”, “processing” and “responsible party”.

The POPIA defines electronic communication as:

“any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;”⁷⁵⁵

One of the avenues for collecting personal information is through electronic communications. The definition of electronic communication in the POPIA, unlike in the Electronic Communications Act, focuses on the information and not on the mode of transmission or collection of the information.⁷⁵⁶ The POPIA is therefore more relevant to communications surveillance of post-surveillance information.

Section 1 of the POPIA defines personal information as any information relating to an identifiable, living, natural or existing juristic person.⁷⁵⁷ Personal information includes

⁷⁵¹ S.2(a) of 4 of 2013; De Bruyn “The Protection of Personal Information (POPI) Act- Impact on South Africa” 2014 13 *International Business and Economics Research Journal* 1315; Neethling *et al Personality Rights* 365, 373; South African Law Reform Project 124, Privacy and Data Protection Report (2009) par 3.2.6.

⁷⁵² Ross “Data Protection Law in South Africa” in Makulilo (ed) *African Data Privacy Laws* (2016) 189.

⁷⁵³ Ss.8-25 of 4 of 2013; Musoni “Is Cybercrimes Search and Seizure under the Cybercrimes and Cybersecurity Bill consistent with the Protection of Personal Information Act?” 2016 *Obiter* 688; S.1 of 4 of 2013 defines a responsible party as “a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information”.

⁷⁵⁴ Neethling *et al Personality Rights* 374. For example, the definition of personal information is helpful in differentiating circumstances where the remedies in POPI Act or common law apply.

⁷⁵⁵ S.1 of 4 of 2013.

⁷⁵⁶ S.1 of 36 of 2005 defines electronic communications as “the emission, transmission or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electromagnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content services”.

⁷⁵⁷ Slabbert and Van der Westhuizen “The Possible Effect of the Protection of Personal Information Act 4 of 2013 on Organ and Tissue Donations” 2017 *Obiter* 632. The personal information of a dead person is not protected by the POPIA.

but is not limited to special information (referred to as private facts in common law), such as sex, race, religious or political affiliations, disability, belief, identifying numbers or symbols, gender and marital status.⁷⁵⁸ The use of the phrase ‘including but not limited to’ in the definition of personal information in the POPIA signifies that the term ‘personal information’ has a wide ambit. It is not limited to the information outlined as referring to personal information in the POPIA. The definition of personal information is wide enough to accommodate more information, for example developments that may be necessary to protect information classified as personal information in the future. This is because the definition is “not limited to” information that are specified in section 1 of the POPIA.⁷⁵⁹

Special personal information is generally prohibited more protection than non-special information because its exposure may result in discrimination against the person to whom it relates.⁷⁶⁰ Special personal information is generally prohibited from being processed, except under certain circumstances or subject to exemptions permitted by the POPIA for example if data subject consents to the processing of such information.⁷⁶¹ The POPIA broadens the purview of the common law by protecting non-private facts as opposed to private facts only.⁷⁶²

The common law does not recognise the disclosure of non-private facts as an invasion of privacy.⁷⁶³ Unlike the common law, the POPIA does not require “an expectation of

⁷⁵⁸ Neethling *et al Personality Rights* 377; S.26 of 4 of 2013 refers to private facts as special personal information.

⁷⁵⁹ S.1 of 4 of 2013.

⁷⁶⁰ Neethling *et al Personality Rights* 391.

⁷⁶¹ Ss.27-33 of 4 of 2013.

⁷⁶² Neethling *et al Personality Rights* 371. The traditional privacy protection under the *actio iniuriarum* does not protect information that is not considered private such as a person’s name or gender however the POPIA protects information, whether it is private, related to an identifiable person in so far as it is being processed. Also, the traditional privacy protection is dependent on a measure of “active control” from the data subject. Modern technology has evolved so much that active control, which depends on the data subject’s awareness of its processing, is nearly impossible. For example, cookies are generated automatically by websites, hence legislation is important to complement the deficiencies of traditional privacy protection; Ross “Personal Data Protection in New Zealand: Lessons for South Africa? 2008 11 *Potchefstroomse Elektroniese Regsblad (PER)* 62.

⁷⁶³ O’ Regan in *NM v Smith* pars [142-143] stated that “it should be emphasised that a court should not lightly conclude that what is a private fact has been rendered a public fact simply because a small number of people may have come to know of it. The question will be one of fact, in particular, whether the fact has been disclosed to such an extent that, viewed objectively, it can no longer, genuinely be considered to be private.” This indicates that had the respondent succeeded in their argument that the disputed facts were not private facts then they would not have been held liable for invasion of the applicants’ privacy; Neethling *et al Personality Rights* 313.

privacy” for the information that it protects.⁷⁶⁴ The common law therefore only protects private facts, while the POPIA protects non-private facts that qualify as personal information in addition to private facts.

The definition of personal information in the POPIA further signifies that both the content and metadata of information obtained from communications surveillance qualify as personal information. This is because the content of a communication and its metadata contain information that could identify the owners of the communication. More often than not, the content of a communication and even its metadata can give a specific description of special information relating to the identified person. The State in utilising communications surveillance is, therefore, a “responsible party” as defined by the POPIA because it processes both personal and special information relating to identified persons.⁷⁶⁵

The POPIA defines “processing of personal information” as:

- “any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
- (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - (b) dissemination by means of transmission, distribution or making available in any other form; or
 - (c) merging, linking, as well as restriction, degradation, erasure or destruction of information;”⁷⁶⁶

The activities outlined in (a)-(c) do not constitute an exhaustive list as the word “including” is utilised. The State engages in the activities in (a)-(c) of the definition when processing personal information in all stages of communications surveillance and such activities should ordinarily be regulated by the POPIA.⁷⁶⁷ However, section 6(c) of the POPIA exempts certain activities of the State from the requirements of the Act.

⁷⁶⁴ *Bernstein v Bester* par [75]; *Khumalo v Holomisa* par [27]; Warren and Brandeis “The Right to Privacy” 1890 (4) *Harvard Law Review* 205; Currie and De Waal *The Bill of Rights Handbook* 298

⁷⁶⁵ S.1 of 4 of 2013 defines a responsible party as “a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information”; Neethling *et al Personality Rights* 368. Neethling *et al Personality Rights* 368; Naude and Papadopoulos “Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments” 2016 1 *THRHR* 190.

⁷⁶⁶ S.1 of 4 of 2013.

⁷⁶⁷ For example, the pre-surveillance stage involves acquiring the surveillance subject’s full names and phone number and presenting it to a judicial officer. S.16(8)(a)(ii) of 70 of 2002.

Section 6(c) of the POPIA provides that processing of personal information by or on behalf of a public body is exempted from the POPIA when:

- “(i) [it] involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety: or
- (ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;”

The exemption granted to the State in terms of section 6(c) of the POPIA is both qualified and unqualified. The exemption pertaining to activities of the State relating to national security, defence, public safety and combatting terrorism (national security matters) is unqualified. This means that once the processing of the personal information of a person is indicated as being for national security matters, the protection in the POPIA does not apply to the person. The South African Law Reform Commission’s (SALRC) justification for recommending a qualified and unqualified exemption in the POPIA is that it aligns with the practices of many developed countries, specifically the practice of the UK as at 2009.⁷⁶⁸

The ECtHR in *Bigbrother Watch v UK* declared the UK’s practices in respect of processing of metadata incompatible with the ECHR.⁷⁶⁹ This indicates that the reasoning underlying the SALRC’s decision has since been declared unlawful in terms of the European regional law. The decision to provide no safeguard for information relating to investigation involving national security matters in the POPIA was thus inspired by a practice in the UK that has since been declared unlawful by the ECtHR.⁷⁷⁰ It is clear that amendment is needed, and that Nigeria must also take cognisance of this development. Article 42 of the SADC Law on Data Privacy (SADC Data Privacy Law) discussed in chapter two permits Member States to limit some of the rights of a data subject for the purpose of the preservation of national security among other purposes.⁷⁷¹ It would be better for Nigeria to implement a law in line with article 42 of the SADC Data Privacy Law rather than the exemption in section 6(c) of the POPIA.

⁷⁶⁸ South African Law Reform Project 124, Privacy and Data Protection Report (2009) 100-101.

⁷⁶⁹ *Bigbrother Watch v UK* par [385].

⁷⁷⁰ *Ibid.*

⁷⁷¹ Chapter 2, sec.2.4.2.

Where the investigation does not relate to national security matters, the exemption from the POPIA only applies where there is an alternative statute that provides adequate safeguards for personal information.⁷⁷² The POPIA therefore applies where the RICA does not provide adequate safeguards for the processing of surveillance information relating to non-national security matters. Section 6 of the POPIA and the inadequate safeguards on personal information in the RICA signify that processing of information relating to national security matters is not statutorily protected.

The common law, in line with provisions of section 8(3)(a) of the Constitution, can provide relief to subjects of surveillance where there is a wrongful disclosure or intrusion of their private facts. The capability of the common law to bridge the *lacuna* in the POPIA and the RICA indicates the invaluable importance of the common law for the protection of privacy. Also, the common law is not rigid. It can be developed to reflect constitutional values.⁷⁷³ It would be preferable, however, for the RICA and the POPIA to be amended.

In Chapter five the thesis explores how Nigerian law can best protect the rights of people impacted on by communications surveillance. The privacy protection regime is constantly changing as a result of rapid innovations in technology and legislation cannot always keep abreast with the changes as constant amendment is problematic.⁷⁷⁴ The flexibility of the common law provides a means in which the courts can give effect to the Constitution in spite of evolving technology.

3.8.4 The Electronic Communications and Transactions Act, 2002

The ECTA was enacted to enable the State to facilitate electronic commerce.⁷⁷⁵ The demands of electronic commerce necessitate legislation in order to assist the economy to evolve in line with global trends.⁷⁷⁶ The ECTA does not provide for

⁷⁷² S.6(c)(ii) of 4 of 2013; Neethling *et al Personality Rights* 378; De Stadler and Esselaar *A Guide to the Protection of Personal Information Act* (2015) 9.

⁷⁷³ *H v Fetal Assessment Centre* 2015 (2) SA 193 (CC) par [67]; Van der Walt and Midgley *Principles of Delict* 99; *Amod v Multilateral Motor Vehicle Accidents Fund (Commission for Gender Equality Intervening)* par [23]; *S v Manamela (Director-General of Justice Intervening)* pars [32-33]; *Beadica v Trustees for the Time Being of the Oregon Trust* 2020 (9) BCLR 1098 (CC) par [71].

⁷⁷⁴ White Paper "Values and the Fourth Industrial Revolution Connecting the Dots Between Value, Values, Profit and Purpose" *Global Agenda Council on Values, University of Stellenbosch Business School (214-2016)* 6.

⁷⁷⁵ S.2(1) of 25 of 2002.

⁷⁷⁶ Swales "An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform- Part Two" 2018 21 *PER* 2; Eislen "Fiddling with the ECT Act - Electronic Signatures" 2014 17 *PELR* 2806.

interception of communications or the acquisition of metadata, but it punishes any unlawful interception of data as a cybercrime. Data is defined in the ECTA as “electronic representations of information in any form”.⁷⁷⁷ The definition of data in the ECTA applies to interception of communication and metadata.

As discussed earlier, the RICA punishes the unlawful interception of communications and the unlawful acquisition of metadata. These crimes are a subset of cybercrimes which are also punishable in terms of the ECTA.⁷⁷⁸ This signifies that punishment for unlawful interception of communications and unlawful acquisition of metadata is fragmented. Cybercrimes are numerous, and as provided in the Cybercrimes Act, they include computer related extortion, fraud and forgery.⁷⁷⁹ Unlawful and intentional interception of data under the ECTA is punishable with a fine of R2, 000, 000 or imprisonment for a period not exceeding 12 months.⁷⁸⁰ The penalty for interception of data in the ECTA is less than the penalty in the RICA.

The Cybercrimes Act punishes the same offence with a fine of R2, 000, 000 and an imprisonment of not lesser than 10 years.⁷⁸¹ Even though the Cybercrimes Act is the latest of the three Acts, it will not take precedence over the ECTA and the RICA in terms on matters relating to targeted surveillance.⁷⁸² This is because the RICA is the primary law on communications surveillance and other laws must defer to it on the matter.⁷⁸³ It, therefore, takes precedence over the ECTA and the Cybercrimes Act in terms of the punishment of unlawful interception of communication.

It is noted that section 35(3)(n) of the Constitution provides that an accused person has the right:

“to the benefit of the least severe of the prescribed punishments if the prescribed punishment for the offence has been changed between the time that the offence was committed and the time of sentencing;”

The ECTA provides a lesser punishment for the unlawful interception of data, namely 12 months’ imprisonment. The RICA and the Cybercrimes Act provide for imprisonment of not less than 10 years and/or a fine of R2, 000,000. An important

⁷⁷⁷ S 1 of 25 of 2002.

⁷⁷⁸ S 86(1) and (2) of 25 of 2002.

⁷⁷⁹ S 87 of 25 of 2002.

⁷⁸⁰ S 89(1) of 25 of 2002.

⁷⁸¹ Ss 49(1) and 51(1)(b)(i) of 70 of 2002; s 19(2) of 19 of 2020.

⁷⁸² *Entabeni Hospital Ltd v Van der Linde / First National Bank of SA v Puckriah* 1994 (2) SA 422 (N) 424.

⁷⁸³ S 2 of 70 of 2002; *AmaBhungane v Minister of Justice* (CC) par [34].

element of section 35(3)(n) of the Constitution is that an accused person can only benefit from a least severe punishment if the punishment for the offence changes between the time of commission and sentencing.

Section 35(3)(n) is not a provision that applies generally to all lesser punishments available in any law, but is specific to a punishment that has been amended. Thus, an accused person may not benefit from a lesser punishment for the same offence in another statute. Sentencing for interception of communications will be meted out on accused persons based on the law under which they are charged. Thus, if an accused persons is indicted under the RICA, they will also be sentenced in line with the RICA even though the ECTA provides a lesser punishment. It would only be where the punishment for the offence under the RICA changes before sentencing that an accused person could benefit from the lesser punishment prescribed, whether in the repealed or amended provision.

Also, the ECTA focuses on the technical operation of electronic communications and transactions. It does not specifically protect the privacy of communications. Instead, it protects the personal information of subscribers of electronic communication.⁷⁸⁴ The principles of processing of personal information, expanded in the POPIA, were first regulated by the ECTA. The principles of electronically processed personal information provided in the ECTA do not apply to data controllers that process data required by any law.⁷⁸⁵ Yet again, the State is exempted from the principles of processing of personal information as set out in the ECTA. The definition of personal information in the ECTA has been amended to reflect the definition in the POPIA.⁷⁸⁶

3.8.5 The Criminal Procedure Act, 1977

Section 205(1) of the CPA provides for the general acquisition of information that may be relevant to a criminal investigation.⁷⁸⁷ Section 205(1) permits a judge of a High Court, a regional court magistrate or a magistrate to summons a person to give

⁷⁸⁴ Marx and O'Brien "To Regulate or to Over-regulate? Internet Service Provider Liability: The Industry Representative Body in terms of the ECT Act and Regulations" 2011 32 *Obiter* 544; Engel "The Role of Law in the Governance of the Internet" 2006 20 *International Review of Law, Computers & Technology* 201.

⁷⁸⁵ S 51 (2), (4) and (6) of 25 of 2002.

⁷⁸⁶ S 110 of 25 of 2002.

⁷⁸⁷ Basdeo, Montesh and Lekubu "Search for and Seizure of Evidence in Cyber Environments: A Law-Enforcement Dilemma in South African Criminal Procedure" 2014 1 *Journal of Law, Society and Development* 56.

evidence. The subpoena is to be granted upon the request of a Public Prosecutor. If the person against whom the subpoena is issued provides the required information before the hearing date, s/he will no longer be required to give evidence in court.⁷⁸⁸ However, Public Prosecutors utilise section 205(1) to circumvent the safeguards in the RICA to acquire communication-related information from CSPs.⁷⁸⁹ Statistics reveal that most metadata acquired are based on a section 205(1) order.⁷⁹⁰

Section 205(1) of the CPA is subject to section 205(4) and section 15 of the RICA. Section 205(4) of the CPA provides for the discretionary power of the court to determine whether the information “is necessary for administration of justice or maintenance of law and order”. The court under section 205(4) has the discretion to determine whether a witness in terms of section 205(1) is a recalcitrant witness.⁷⁹¹ The relationship between section 15 of the RICA and section 205(1) of the CPA is the focus of this section. Section 15 of the RICA provides that procedures in alternative statutes may also be utilised to acquire communication-related information which are not for an “on-going basis”.

The utilisation of section 205(1) of the CPA in this manner is unlawful on two grounds. Firstly, the CSPs are prohibited from accessing the information stored on their networks without their customer’s consent or without a surveillance direction.

⁷⁸⁸ S.205(1) of 51 of 1977.

⁷⁸⁹ Duncan *Stopping the Spies* 90; The heads of argument of the 1st Applicant pointed out how the SAPS and the NPA utilised section 205 of 51 of 1977 to seize the phone records of Journalist Athandiwe Saba. However, the validity of a section 205 warrant was not in contention in *AmaBhungane v Minister of Justice* https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf (accessed 2020-08-10) par [204.2]. It can also be argued that some processes are time consuming and although they may lack the safeguards provided for in RICA, they are aimed at ensuring an investigation in a timeous manner. The affected party should have recourse through post-surveillance notification, if the investigation was malicious and/or there were no reasonable grounds. The time frame in which post-surveillance notification should be provided will have to be determined on a case-by-case basis.

⁷⁹⁰ Daily Maverick reported that most of the court orders received by Vodacom in the 2016/17 financial year to submit evidence of acquisition of metadata were issued in terms of s.205 of Act 51 of 1977 court orders. The statistic shows that in terms of the RICA there were 1,075 interception orders received and there were 19, 850 court orders in terms of s. 205 of 51 of 1977; Swart “Your Cellphone Records and the Law: The Legal Loophole that lets State Spying Run Rampant” *Daily Maverick* (20 May 2018) <https://www.dailymaverick.co.za/article/2018-05-20-your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/> (accessed 2019-06-21); Duncan *Stopping the Spies* 92; Watney “State-On-Nationals’ Electronic Communication Surveillance in South Africa: A Murky Legal Landscape to Navigate?” (2015) https://digifors.cs.up.ac.za/issa/2015/Proceedings/Full/3_Paper.pdf (accessed on 2020-01-10).

⁷⁹¹ S.189 of 51 of 1977. A recalcitrant witness is a witness who refuses to be sworn, make an affirmation or refuses to answer any question after being sworn. This is different from a hostile witness, in section 190(2), who provides evidence that is “adverse to the person calling him”.

Secondly, section 205(1) of the CPA is not an alternative statute with a procedure for the acquisition of communication-related information as envisaged by section 15(1) of the RICA. Concerning the eligibility of the CSPs, the Public Prosecutor relates to CSPs as persons who are likely to give material information to an alleged offence. This assessment is incorrect. The CSPs do not possess material information for investigation because they are not lawfully permitted to access customers' communications or its metadata except with the customer's consent or if there is a surveillance direction addressed to them.⁷⁹² Nevertheless, the CSPs seems to give in to the Public Prosecutor in order to avoid court appearances as the statistics of the surveillance order obtained through the CPA indicate.⁷⁹³ The information that CSPs can provide in this regard is whether the accused person's metadata is stored on their network. Thereafter, the Public Prosecutor can acquire communication-related information in line with the procedures in section 17 and 19 of RICA or any other statute providing procedures for the acquisition of metadata.

In addition, the term "subject to" in section 205(1) means that the provision is conditional or dependent on, section 15(1) of the RICA, as opposed to being exempted therefrom. This means that section 205(1) must align with the objects of the RICA which is to safeguard rights in the event of surveillance. This is not to say that the RICA safeguards rights adequately, but that the minimal safeguards in the RICA are not to be discarded at the convenience of the State.

Furthermore, the Constitutional Court in *Nel v Roux NO* ruled that a just excuse for refusal to furnish information as a witness includes an infringement of the witness' fundamental rights.⁷⁹⁴ The judicial officer, in line with section 205(4) of the CPA, has a discretionary power to determine whether there is a just cause to refuse to give evidence. The subpoenas should therefore ordinarily be regarded as an opportunity for CSPs to inform the court of the reasons for their refusal to give evidence, which would usually be the preservation of their customer's rights, as CSPs are responsible for the protection of the privacy of their customers.⁷⁹⁵ The subpoena should not, but

⁷⁹² Ss.12-14 of 70 of 2002.

⁷⁹³ Swart "Your Cellphone Records and the Law: The Legal Loophole that lets State Spying Run Rampant" *Daily Maverick* (20 May 2018) <https://www.dailymaverick.co.za/article/2018-05-20-your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/> (accessed 2019-06-21)

⁷⁹⁴ 1996 (4) BCLR 592 (CC) par [9].

⁷⁹⁵ This is because CSPs have a fiduciary relationship with their customers in which the former is required to protect the latter's privacy. Also, the nature of the relationship with the Electronic

for the inadequate understanding of the RICA, be a threat to CSPs. Nigeria should thus bear in mind that education of CSPs on the existing communications surveillance statutes is important for the protection of the guaranteed rights.

On the second ground, the provision of section 205(1) of the CPA is a procedure for examination of a witness who may possess material information related to an alleged crime. The CPA does not provide procedures for the acquisition of metadata and so does not qualify as one of such other statutes referred to in section 15(1) of the RICA. Therefore, the acquisition of metadata through section 205(1) of the CPA is unlawful.

Finally, on the relationship between the RICA and the CPA, the latter statute was enacted before the Constitution and has been amended in line with the RICA. There is a constant renegotiation of the powers of the State to align with the rights in the Bill of Rights.⁷⁹⁶ The court as the final arbiter between the State and the people must interpret statutes that limit the rights in the Bill of Rights in light of the Constitution. It is counter-productive to the mandate of respecting, protecting, promoting and fulfilling the rights in the Bill of Rights to protect rights through a statute (RICA) and then disregard the protection through another statute (CPA).⁷⁹⁷

The tension between section 15 of the RICA and section 205 of the CPA is a problem. Nigeria should aim to avoid vague and conflicting laws as she develops her legal framework on communications surveillance. Vagueness in the composition of statutory provisions can lead to an interpretation that undermines the purpose and objects of the statute and unjustifiably infringes on rights.

Service Providers and their users is such that there is no assumed risk that data will be transferred to a third party; See the progress in decisions from the Supreme Court from *Smith v Maryland*, 442 U.S 735 (1979); *Carpenter v United States*, 22 June 2018, 585 U.S (2018) par [3,11]; Chaudhari & Prasad “*Carpenter v United States: State Surveillance and Citizen Privacy*” 2019 13 *National Academy of Legal Studies and Research (NALSAR) Student Law Review* 130. In *Carpenter v United States*, the State obtained the accused person’s metadata through a court order pursuant to the Stored Communications Act, 1986 and not a warrant under the Fourth Amendment. The standard requirement for obtaining evidence under the Stored Communications Act is lower than that required to procure a warrant for a Fourth Amendment search and seizure. The Supreme Court of the United States held that the State’s action was a warrantless search and therefore unreasonable thus violating the appellant’s Fourth Amendment rights. The Supreme Court of the United States ruled in favour of the law with a higher propensity for the protection of right.

⁷⁹⁶ Chaudhari and Prasad “*Carpenter v United States: State Surveillance and Citizen Privacy*” 2019 13 *National Academy of Legal Studies and Research (NALSAR) Student Law Review* 130.

⁷⁹⁷ S.7 of the Constitution; *Independent Institute of Education (Pty) Limited v Kwazulu-Natal Law Society* 2020 (4) BCLR 495 (CC) par [38].

3.8.6 The Cybercrimes Act, 2020

The Cybercrimes Act⁷⁹⁸ was drafted to provide for the investigation, prosecution and prevention of cybercrimes.⁷⁹⁹ Initially it was drafted as the Cybercrimes and Cyber Security Bill. However, much criticism was raised towards the provisions on cyber security because of the extensive powers afforded to the State which infringed the right to freedom of expression.⁸⁰⁰ As a result, the provisions relating to cybersecurity were removed and the Cybercrimes Act was enacted in 2021.

Unlike the RICA that protects communication transmitted over a network only, the Cybercrimes Act protects information in an electronic form and the electronic device itself from unlawful access.⁸⁰¹ **The Cybercrimes Act defines “data” as “electronic representations of information in any form”.**⁸⁰² So, information stored on phones and computers, for example pictures, text messages, e-mails, are referred to as data and anyone who unlawfully and intentionally accesses such data is guilty of a cybercrime.⁸⁰³ Like the RICA, any person who unlawfully acquires data that is transmitted to or from a computer system is guilty of an offence punishable with 10 years’ imprisonment or to both imprisonment and a fine.⁸⁰⁴

The Cybercrimes Act not only prohibits unlawful interception of data, but also any interception of electromagnetic emissions from a computer system.⁸⁰⁵ The Cybercrimes Act thus protects data from an electronic device and any signals being emitted from the device. It protects the privacy of the user of an electronic device by prohibiting unlawful interference with such device. The Act furthermore provides for

⁷⁹⁸ Cybercrimes Act 19 of 2020.

⁷⁹⁹ Van Niekerk “The Cybersecurity Dilemma: Considerations for Investigations in the Dark Web” 2018 31 *Acta Criminologica: South African Journal of Criminology* 133; Stallin and Brown *Computer Security: Principles and Practice* 4ed (2018) 601-602. Cybercrime is defined as “criminal activity in which computers or computer networks are a tool, target, or a place of criminal activity” Centre for Advanced Studies in Science and Technology (2009) UNIT 01: <http://www.information-retrieval.info/cybercrime/index01.html> (accessed on 2020-10-01).

⁸⁰⁰ Comments of the Law Society of South Africa (LSSA) on Cybercrimes and Cybersecurity Bill <https://www.lssa.org.za/wp-content/uploads/2020/01/LSSA-CYBERCRIMES-AND-CYBERSECURITY-BILL-Comm> (accessed on 2020-10-10) 1-7.

⁸⁰¹ S 2 of 19 of 2020.

⁸⁰² **S 1 of 19 of 2020**; S 1 of 25 of 2002 gives data a broader definition by including any information in an electronic form as data.

⁸⁰³ S 2 of 19 of 2020. The offence relating to unlawfully securing access of a computer device, program, storage or the information stored is punishable with an imprisonment of not more than five years.

⁸⁰⁴ S 3(1)(a) and (b) and S.14 of 19 of 2020.

⁸⁰⁵ S 3(2) of 19 of 2020.

more offences for unlawful interception of communication than the RICA.⁸⁰⁶ It expands the offence of unlawful interception of indirect communication in the RICA. In addition to criminalising interception of data, the Act also creates offences for possession of such data. Any person possessing data that is suspected to be unlawfully acquired and who is unable to provide a “satisfactory exculpatory account” is guilty of an offence.⁸⁰⁷ Thus, possession of unlawfully acquired data is a cybercrime.

The Cybercrimes Act updates the technical terminology in the RICA by exchanging the term “telecommunications service provider” with “electronic service provider”.⁸⁰⁸ The Cybercrimes Act, however, refers to the interception of indirect communication in terms of the RICA as interception of data. This causes confusion because the RICA separates indirect communications into content of communication and communication-related information.⁸⁰⁹ Also, these two categories of indirect communications have different procedures afforded to their interception.⁸¹⁰ The term “interception of data” as utilised in the Cybercrimes Act does not clearly delineate the differences in the interception of communication and acquisition of communication-related information.

The absence of synergy of provisions relating to the interception of communications between the Cybercrimes Act and RICA is problematic. Nigeria in avoiding this problem in developing her legal framework on communication surveillance should endeavour to synergise the new provisions with existing laws as this reduces conflicts of laws and aids the interpretation of laws.⁸¹¹

⁸⁰⁶ Ss 3(2) and (3) of 19 of 2020.

⁸⁰⁷ S.3(3) of 19 of 2020.

⁸⁰⁸ S.38 of 19 of 2020.

⁸⁰⁹ *Ibid.*

⁸¹⁰ Chapter 1, Part A and B of 70 of 2002.

⁸¹¹ Another law that was formulated on communications surveillance is the COVID-19 contact tracing policy. This law was formulated in terms of the Disaster Management Act No.57 of 2002 by virtue of Chapter 3 of the GN 43199. The Disaster Management Act is applicable during a disaster only. The COVID-19 contact tracing policy regulates contact tracing by electronic means. It was assumed that this procedure will enable the State to identify persons who has been in close contact with an infected person. The COVID-19 Contract tracing law was discontinued because the surveillance technology could not ascertain the exact proximity of the devices that are tracked. It thus failed to meet the section 36(1)(d) of the Constitution requirement for justifying the purpose of the limitation.

3.9 Summary of the main features of legislative framework of communications surveillance in South Africa

A brief summary of the South African legislative framework on communications surveillance is now provided to link the South African law to the thematic problem areas identified in chapter one in the Nigerian law regulating communications surveillance. The purpose of the summary is to link the comparable South African law to the existing Nigerian law, which is discussed in the next chapter, and to the reforms which are proposed in chapter five. The reader will recall that four broad problematic areas were identified in chapter one. These are: the lack of a comprehensive statute for communications surveillance; ineffective procedural guidelines for the collection of content and metadata; inadequate oversight mechanisms; and little recourse for surveillance subjects because of the missing requirement for post-surveillance notification.

It has been shown in this chapter that in South Africa there is a single and comprehensive law regulating communications surveillance, namely the RICA. Whilst there are other laws which deals with communications surveillance, such as the ECTA, CPA and POPIA, the provisions in these statutes addressing communications surveillance are incidental to their aims. The ECTA, CPA and POPIA also refer to the RICA as the primary overarching law on communications surveillance. The RICA supersedes in the event of conflict, which ensures clarity and specificity on the position of which law applies in matters relating to communications surveillance.

The South African legislative framework provides detailed procedural guidelines for the authorisation of an intercept warrant through the RICA. Chapter five will explore whether this procedure for the execution of communications surveillance should be recommended for implementation in Nigeria. The various loopholes identified in the RICA such as technical and infrastructural difficulties relating to the implementation agency and the unnecessary disclosure of information not required for investigation, were flagged in this chapter to ensure that Nigeria adequately addresses such issues in its reformed legislative framework.

In South Africa, judges have oversight over communications surveillance. The designated judge is authorised to grant an interception warrant for the execution of communications surveillance in respect of the content of the communication. Plus, the

application for the acquisition of metadata is presided over by a judge or a magistrate. Whilst some aspects of the South African system are worthy of emulation, the oversight mechanisms in South Africa are problematic. For this reason, in *AmaBhungane*, the Constitutional Court held that the procedures in the RICA relating to the appointment of the designated judge resulted in a lack of independence. Another problem was that judicial officers do not always have the requisite expertise and training required to handle the peculiarity of an interception order. When exploring reform for Nigeria, the constitutional challenge in *AmaBhungane* will be considered to propose viable oversight mechanisms for Nigeria.

Unfortunately, the laws regulating communications surveillance in South Africa do not provide for post-surveillance notification. This problem formed the basis of a separate challenge to the RICA in *AmaBhungane*. The Constitutional Court rectified the position and held that LEOs must notify surveillance subjects of the surveillance within ninety days of the conclusion of the investigation, provided that post-surveillance notification does not jeopardise the investigation. This measure provides a balance between the protection of the right to privacy of the surveillance subject and the need for LEOs to perform their criminal justice duties and will be used to formulate an appropriate framework for Nigeria.

3.10 Conclusion

The right to privacy in South Africa is protected by the Constitution, together with the common law and through statute. The Constitution recognises specifically the right to communications privacy by prohibiting the privacy of communications from infringement. The right to privacy, like other rights in the Bill of Rights, is subject to limitation in section 36 of the Constitution that provides for laws which limit rights to be reasonable and justifiable in an open and democratic society. The Constitution further provides that rights conferred by common law and statute must be consistent with the Bill of Rights and be interpreted and developed in accordance with the spirit, purport and objects of the Bill of Rights. The protection and limitations of the right to privacy in common law and statutes must therefore conform with the Bill of Rights.

Communications surveillance in South Africa is primarily regulated by the RICA. Given that the RICA infringes the right to privacy, such limitation must be reasonable and justifiable in accordance with the requirements in section 36 of the Constitution.

Particular problems with the RICA are the authorisation and the execution of communications surveillance, in addition to the processing of post-surveillance information. In *AmaBhungane* the Constitutional Court, when asked to confirm the High Court's order of constitutional invalidity, used the section 36(1) factors as a guide and declared sections in the RICA unconstitutional to the extent that they failed to provide adequate safeguards for the right to privacy and other rights. Section 36(1) of the Constitution ensured that paramount protection was afforded human rights through a balancing process. This indicates the importance of providing guiding principles to aid the court in its limitation of rights adjudication. The Constitutional Court applied this balancing process when analysing sections 1 (appointment of judges), 16 (procedure for authorisation of surveillance, 35 and 37 (both sections provide for post-surveillance processing) of the RICA.

The absence of measures securing the independence of the designated judge in the RICA was one of the grounds for the invalidity of the RICA as the Minister of Justice is responsible for the appointment and the term of office is unspecified in the Act. The Constitutional Court further declared the RICA invalid to the extent that it failed to provide: (a) adequate safeguards to protect the rights to a fair hearing as a result of the *ex parte* nature of the communications surveillance application and direction; (b) post-surveillance notification, which was an unjustifiable infringement on the right of access to court; (c) inadequate safeguards for the processing of surveillance information; (d) adequate safeguards to protect the communications of legal practitioners and journalists, which was an unjustifiable infringement to the rights to a fair trial and fair hearing.

Parliament was ordered to amend the RICA within 36 months of the date of the judgment, with the Court providing interim relief until this occurs. Two new provisions were inserted in the RICA, providing for disclosure to the designated judge where the surveillance subject is a legal practitioner or a journalist and post-surveillance notification after 90 days of the date of expiry of the communications surveillance order.

In spite of the commendable decision in *AmaBhunagane*, there are still issues that are yet to be addressed in the communications surveillance regime in South Africa. The provisions of the RICA indicate an inadequate understanding of the intrusive nature of metadata. The CPA, for example, is being utilised as an alternative statute to acquire

communication-related information. Also, LEOs are permitted to dispense with a communications surveillance order if they are a party to communications. Furthermore, the RICA permits other laws to regulate communications surveillance in prisons. It is hoped that these issues will be rectified when parliament amends the RICA.

This chapter has demonstrated that South Africa's communications surveillance regime provides a valuable comparator for Nigeria. Although South Africa's legislative framework needs improvement, the courts' approach when addressing many of the problems in the RICA is insightful. The South African legal framework on the right to privacy and communications surveillance when considered holistically, that is, taking into cognisance the High Court and Constitutional Court's decisions on the RICA, the Constitution and the common law protection for privacy, provides an excellent comparator for the development of the Nigerian legal framework on communications surveillance. The next chapter turns to Nigeria.

CHAPTER FOUR

THE LEGAL FRAMEWORK OF COMMUNICATIONS SURVEILLANCE IN NIGERIA

4.1 Introduction

Chapter two analysed the international and regional (African and European) law on the right to privacy generally and specifically on communications surveillance. Chapter three explored the South African jurisprudence on the right to privacy and communications surveillance. These chapters also serve as a benchmark for the analysis of Nigeria's legal framework on communications surveillance.

This chapter discusses the current legal framework of communications surveillance in Nigeria. First, it explores the legal position on the right to privacy and the limitation of rights in the Constitution of the Federal Republic of Nigeria, 1999 (1999 Nigerian Constitution). The chapter also provides a brief history of the Nigerian Constitution in order to contextualise the 1999 Nigerian Constitution and, compare it to the South African Constitution and the common law protection of privacy in South Africa.

Secondly, the chapter investigates the common law position on the protection of privacy in Nigeria. Thereafter, the laws regulating communications surveillance in Nigeria are examined. It reveals a mix of statutes and mainly subordinate legislation as the framework for regulating communications surveillance which involves processes before, during and post-surveillance. The chapter concludes with a summation of the analysis and indicates that the Nigerian legal framework on communications surveillance is flawed and does not adequately protect and safeguard fundamental rights.

4.2 Brief history of the Nigerian Constitution

This section clarifies how the current 1999 Nigerian Constitution, especially its Bill of Rights, came into existence. It also posits the reasons for the inadequacies in the Bill of Rights and why so little attention has been given to amending the Bill of Rights to align it with international treaties, in spite of Nigeria's ratification of these.

Nigeria became a unified country after the amalgamation of the Northern and Southern Protectorates of Nigeria in 1914.⁸¹² The amalgamation was a response to the colonial

⁸¹² Akinola "Nigeria: The Quest for a Stable Polity: Another Comment" 1988 87 *African Affairs* 441.

government's need for administrative efficiency so as not to offset the deficit accruing from the management of the Northern protectorate with British finances.⁸¹³ As a result, in 1914, under the governorship of Lord Fredrick Lugard, the British colonialists decided to offset the Northern protectorate's deficit with the surplus in the Southern protectorate by merging the two protectorates.⁸¹⁴ Lugard ruled Nigeria by a system known as indirect rule with the country administered through its traditional rulers.⁸¹⁵ Hugh Clifford became governor-general after Lugard and sought to provide a structure for Nigeria through a Constitution. Several Constitutions were drafted following Clifford's style of governance and were named after the incumbent Governor-Generals.⁸¹⁶

The Clifford's Constitution of 1922, Richard's Constitution of 1946, Macpherson's Constitution of 1951, Lyttleton's Constitution of 1954 and the Independence Constitution of 1960 all saw Nigeria as a colony under the British Empire.⁸¹⁷ The 1963 Nigerian Constitution declared Nigeria as a Republic and fully independent of the British empire thereby replacing the Privy Council with the Nigerian Supreme Court as the highest appellate court in Nigeria and removing the Queen of England as Nigeria's Constitutional monarch.

The independence of Nigeria from colonialism marked the beginning of freedom from the oppression of colonial masters whose rule "gagged" fundamental rights.⁸¹⁸ Incorporating human rights in the Constitutions was a precaution to prevent such oppression from occurring in the future. Unfortunately, the freedom was short-lived. In 1966, military dictators perpetrated oppression by taking power from democratically elected leaders and ignored human rights.

Nigeria continued rewriting and amending its Constitutions from the 1960 Constitution under the colonial government, through the military dictatorship and under the current

⁸¹³ Udombana *Constitutional Restructuring in Nigeria: An Impact Assessment* Public Lecture delivered at 'Change Nigeria' conference, Lagos, Nigeria (25 April 2017) 7.

⁸¹⁴ Udombana, Public Lecture delivered at 'Change Nigeria' conference 4; Maier, *This House Has Fallen: Nigeria in Crisis* (2002)7; Diala "The Dawn of Constitutionalism in Nigeria" in *Constitutionalism and democratic governance in Africa: Contemporary perspectives from sub-Saharan Africa* in Mbondenyi and Ojienda (eds.) (2013) 138.

⁸¹⁵ Whitaker *The Politics of Tradition, Continuity and Change in Northern Nigeria, 1946-1966* (1970) 27.

⁸¹⁶ Diala "The Dawn of Constitutionalism in Nigeria" 138.

⁸¹⁷ *Ibid.*

⁸¹⁸ *Inspector General of Police (IGP) v All Nigerian Peoples Party (ANPP)* (2007) LPELR-8217 (CA) 41.

democratic government.⁸¹⁹ Nigeria operates a federal system of government. It has 36 federating states and a federal capital territory.⁸²⁰ Most constitutional amendments focussed on matters such as the creation of federating states and local governments, rather than the improvement of the Bill of Rights. The post-colonial amendments to the Nigerian Constitution focused more on rehabilitating the power dynamics between the British government and Nigeria or among the different geopolitical zones of Nigeria.

Currently, the 1999 Nigerian Constitution (as amended) is in force and has been amended thrice. This Constitution is popularly referred to as the 1999 Nigerian Constitution (as amended) to signify that there have been alterations. The current Constitution will be referred to as the 1999 Nigerian Constitution in this thesis and where there is a need to refer to the various alterations, these will be specifically stated.

The 1999 Nigerian Constitution is not a statute, but a foundational document that provides a framework for the enactment of statutes and other laws, even though it has been criticised often as the product of a military decree (Decree 24 of 1999) which does not reveal the will of the people. Critics of the 1999 Nigerian Constitution have classified the preamble, “We the people”, as false.⁸²¹ Nevertheless, the 1999 Constitution was a replica of the 1979 Constitution, one that enjoyed large participation by Nigerians.⁸²² The 1979 Constitution was deliberated by a Constituent Assembly consisting of experts in law, political science, economics, history and other social sciences.⁸²³ The 1999 Nigerian Constitution, being a replica of the 1979 Constitution, therefore, reflects the will of the people.

This is not to say that the 1999 Nigerian Constitution is perfect and, as will be discussed below, its protection of the right to privacy and the manner in which it limits rights is inadequate. Also, the 1999 Nigerian Constitution was imposed by the military government that ushered in the democratic government in 1999. Nonetheless, the provisions of the 1999 Nigerian Constitution were, in principle, the will of the people at the time of its promulgation.

⁸¹⁹ The 1999 Constitution of the Federal Republic of Nigeria (as amended).

⁸²⁰ S.2(2) of the 1999 Nigerian Constitution.

⁸²¹ Udombana Public Lecture delivered at ‘Change Nigeria’ conference 7.

⁸²² Diala “The Dawn of Constitutionalism in Nigeria” 140; Oyediran *The Nigerian 1979 Elections* Macmillan International College Editions: Contemporary African Issues Series (1981) 10.

⁸²³ *Ibid.*

4.3 Supremacy of the 1999 Nigerian Constitution

The preamble to the 1999 Nigerian Constitution states the purpose of the Constitution as:

“providing for good government and welfare of all persons in our country, on the principles of freedom, equality and justice, and for the purpose of consolidating the unity of our people.”

The interpretation of the provisions of the Constitution must be in line with its purpose. The principles of freedom, equality and justice must be paramount in constitutional interpretation. This is similar to the role of the constitutional values in the South African Constitution.⁸²⁴

Section 1(1) of the 1999 Nigerian Constitution provides for the supremacy of the Constitution and provides that it shall have a “binding force on the authorities and persons throughout the Federal Republic of Nigeria”.⁸²⁵ The 1999 Nigerian Constitution binds everyone in Nigeria including the State, individuals and juristic persons.⁸²⁶ All laws in Nigeria also derive their validity from the 1999 Nigerian Constitution. Any law that is inconsistent with the provisions of the 1999 Nigerian Constitution is void to the extent of its inconsistency.⁸²⁷

Nigerian Constitutions under the colonial era and under the military regimes were not always the supreme law of the land. The Constitutions in the colonial and the military eras were subject to the British government and the Head of State respectively. The Constitutions in operation during the colonial era and the military era did not attempt to protect human rights because they were forced upon the people to achieve political subjugation. This is not surprising because colonialism and military dictatorship are “antithetical” to human rights protection.⁸²⁸ It is thus important to ensure that, communications surveillance is regulated and lawful in order to prevent Nigeria from slipping back into its dictatorial past under the guise of democracy.

The 1999 Nigerian Constitution also provides for the separation of powers between the executive, legislature and the judiciary in order to provide for checks and balances.

⁸²⁴ S.1(1) of the Constitution of the Republic of South Africa, 1996.

⁸²⁵ S.1(1) of the 1999 Nigerian Constitution.

⁸²⁶ *IGP v ANPP*, 43; *Osha v Phillips* (1972) 4 SC 259; *A.G Abia State v A.G Federation* (2002) 6 NWLR (Pt. 763) 264; *Ifegwu v Federal Republic of Nigeria* (2001) 13 NWLR (Pt. 229) 103; *Ikine v Edjerode* (2001) 18 NWLR (Pt. 725) 446.

⁸²⁷ S.1(3) of the 1999 Nigerian Constitution.

⁸²⁸ Dada “Human Rights under the Nigerian Constitution: Issues and Problems” 2012 2 *International Journal of Humanities and Social Sciences (IJHSS)* 35.

These arms of government are to execute, enact and interpret laws respectively.⁸²⁹ The purpose of separation of powers is to ensure that no arm of government has too much power and becomes a tyranny.⁸³⁰ The legislature consists of the National Assembly, that is, the Senate (upper legislative house), and House of Representatives (lower legislative houses) and the Houses of Assembly that enact laws for the federating states.⁸³¹ This structure of various legislative houses represents the nature of a federal system of government.

Statutes enacted by the National Assembly prevail over those of the federating states.⁸³² In addition, there are some matters that can only be enacted exclusively by the National Assembly.⁸³³ These matters, such as defence, evidence, military, police and government security agencies, quarantine, wireless broadcasting and “any matter incidental or supplementary to any matter mentioned in this list”, are listed in the Exclusive Legislative List.⁸³⁴ This indicates that matters in the Exclusive Legislative List or incidental to them cannot be delegated to the executive through subordinate legislation. The 1999 Nigerian Constitution also refers to the laws enacted by the National Assembly as Acts and those enacted by the State House of Assembly as Laws. The classification of the enactment of different legislative houses causes some interpretative problems with section 45 of the 1999 Nigerian Constitution and is discussed in section 4.6 below.

The judiciary interprets the laws and determines questions relating to the civil rights and obligations of all persons and the State.⁸³⁵ The judiciary is “...the guardian of our rule of law and the midwife of our legal system...”⁸³⁶ Where there is a word that is not defined in the 1999 Nigerian Constitution or other statutes, it is the duty of the Court

⁸²⁹ S.4(1) of the 1999 Nigerian Constitution.

⁸³⁰ Kalu “Separation of Powers in Nigeria: An Anatomy of Power Convergences and Divergencies” 2018 9 *Nnamdi Azikiwe University Journal of International Law and Jurisprudence (NAUJILJ)* 117; Malemi *Administrative Law* 3ed (2008) 56-57; Ojo “Separation of Powers in a Presidential System of Government” 1981 *Public Law Journal* 105; *Myers v United States* (1962) 272; Ikongbeh “Separation of Powers under the Constitution of Nigeria 1999: A Critical Review of its Application since 29th May, 1999” 2003 1 *Nigeria Law Journal* 92; Okeke *Introduction to Consular Immunities and Privileges, Jurisprudence and Constitutional Law* (2010) 195.

⁸³¹ S.4(6) of the 1999 Nigerian Constitution.

⁸³² S.4(5) of the 1999 Nigerian Constitution.

⁸³³ S.4(3) of the 1999 Nigerian Constitution.

⁸³⁴ Part 1 of the second schedule to the 1999 Nigerian Constitution.

⁸³⁵ S.6(6)(b) of the 1999 Nigerian Constitution.

⁸³⁶ *Nwali v Ebonyi State Independent Electoral Commission* (2014) LPELR-23682 (CA) 63.

to interpret it by providing a broad definition that conveys its intent and underlying policy and purpose.⁸³⁷

The Supreme Court⁸³⁸ commented on the interpretation of the Constitution as follows:

“One of the principles suitable to its *sui generis* nature is that it must be given a benevolent, broad, liberal and purposive interpretation and a narrow, strict, technical and legalistic interpretation must be avoided to promote its underlying policy and purpose”.⁸³⁹

The courts have often referred to precedent from international law and foreign courts that utilise similar words or phrases while defining terms.⁸⁴⁰ The Court of Appeal held that statutes that are domesticated from international law will prevail where there is a conflict with other statutes.⁸⁴¹ “It is presumed that the legislature does not intend to breach an international obligation”.⁸⁴² Courts have also often referred to Blacks’ law dictionary, among others, in determining the legal meaning of words.⁸⁴³

4.4 The Bill of Rights in the 1999 Nigerian Constitution

Nigeria became an independent State from British rule on October 1, 1960 and thereafter produced the first Nigerian Constitution (1960 Constitution) at independence. A Bill of Rights was included in the Constitution for the first time in 1960.⁸⁴⁴ The purpose of the inclusion of human rights into the 1960 Constitution was to assure the minority groups of Nigeria of the protection of their human rights after independence from colonial rule.⁸⁴⁵ The Bill of Rights has remained largely unchanged

⁸³⁷ *Minister of Home Affairs v Fisher* (1972) 2 WLR 899 319, 328; *Abdulkarim v Incar (Nig) Ltd* (1992) NWLR (Pt. 251) 1; *Bronik Ltd v WEMA Bank Ltd* (1983) All NLR 272; *Nwali v Ebonyi State Independent Electoral Commission* 31-32.

⁸³⁸ In Nigeria, the Supreme Court is the highest in hierarchy followed by the Court of Appeal then the High Court.

⁸³⁹ *Rabiu v Kano State* (1980) 8 11 SC (Reprint) 85.

⁸⁴⁰ *Nwali v Ebonyi State Independent Electoral Commission* 62, 64.

⁸⁴¹ *Abacha v Fawehimi* (2000) 6 NWLR (Pt. 660) 228.

⁸⁴² *Ibid.*

⁸⁴³ *Nwali v Ebonyi State Independent Electoral Commission*, 56-57.

⁸⁴⁴ Ss.17-32 of the 1960 Constitution provided for fundamental human rights; Sanni “Fundamental Rights Enforcement Procedure Rules, 2009 as a tool for the enforcement of the African Charter on Human and Peoples’ Rights in Nigeria: The Need for Far-reaching Reform” 2011 11 *African Human Rights Law Journal (AHLJ)* 513-515; Brems and Adekoya “Human Rights Enforcement by People Living in Poverty: Access to Justice in Nigeria” 2010 54 *Journal of African Law (JAL)* 2. The powers of the states were predominantly shouldered by three regions: the Eastern, Northern and the Western Nigeria. As a result, demographically smaller regions became fearful of a potential arbitrary use of power and domination by the majority. Consequently, fundamental human rights were included in the 1960 Constitution to allay these fears. Ajomo “Human Rights under the Nigerian Constitutions” in Osinbajo and Kalu (eds) *Democracy and the Law* (1991) 106-107.

⁸⁴⁵ Anucha *The Impact of Constituent Assemblies (1978-1995) on Nigerian Constitutions and Political Evolution* (doctoral thesis, Department of Political Science, Clark Atlanta University) July

since the 1960 Constitution up until the current Constitution, that is, the 1999 Nigerian Constitution and in particular, the provision on the right to privacy has remained substantially the same.

Although Nigeria is a signatory to the ICCPR, ICESCR, CRC and other treaties, both regional and subregional, all of which protect human rights, the Bill of Rights has not been amended to reflect these treaty obligations. For example, the right to privacy as provided for under the 1999 Nigerian Constitution is discriminatory and contrary to UDHR and ICCPR as its protection is only guaranteed for Nigerian citizens.⁸⁴⁶ This is discussed in section 5 of this chapter. Hence, the Bill of Rights does not protect human rights to the extent that international law requires. Also, the availability of fundamental rights in national constitutions does not signify the State's adherence or commitment to its fulfilment.⁸⁴⁷ The 1999 Nigerian Constitution is therefore deficient because of its non-alignment with international law.

It is also shown that judges struggle to interpret and apply the Bill of Rights in a manner that effectively safeguards human rights. This necessitated the introduction of a Regulation by the Chief Justice that urges the application of international law in human rights adjudication through the Fundamental Rights Enforcement Procedure Rules, 2009 (FREPR). The FREPR is a Regulation formulated by the Chief Justice, empowered by section 46 of the 1999 Nigerian Constitution to improve court procedures regarding human rights adjudication.⁸⁴⁸ The FREPR enables judges to consider the International Bill of Rights in human rights adjudication even though there is not yet provision for it in a statute. This indicates the judiciary's acknowledgement that the 1999 Nigerian Constitution is defective to the extent that it does not incorporate international law.

2010;The first and second phase of the constitution-making exercise was under the colonial government and there were six Constitutions prior to the 1963 independence Constitution and they are: the Constitution of 1914 that created the British colony named Nigeria; the Clifford Constitution, 1922, Richard's Constitution, 1946, Macpherson's Constitution, 1951; Lyttelton's Constitution, 1954;Constitution of Nigeria, 1960.

⁸⁴⁶ S.37 of the 1999 Nigerian Constitution.

⁸⁴⁷ Sanni "Fundamental Rights Enforcement Procedure Rules, 2009 as a tool for the enforcement of the African Charter on Human and Peoples' Rights in Nigeria: The Need for Far-reaching Reform" 2011 11 *AHRLJ* 512; Brems and Adekoya 2010 54 *JAL* 258; Udombana 2005 5 *Interpreting Rights Globally: Courts and Constitutional Rights in Emerging Democracies*" *African Human Rights Law Journal (AHRLJ)* 55.

⁸⁴⁸ Commencement of the FREPR.

The courts have often stressed the importance of the Bill of Rights by stating that fundamental rights are “the bedrock for a free society devoid of forces of unbridled aggression, oppression, repression, [and] authoritarianism”.⁸⁴⁹ As a result, the judiciary have interpreted section 46 of the 1999 Nigerian Constitution as empowering the judiciary to ensure the court is well-positioned to effectively dispense justice in human rights cases. Section 46 of the 1999 Nigerian Constitution provides redress in the High Court as the court of first instance for anyone whose fundamental right “has been, is being or likely to be contravened”. The court has deemed it fit to uphold this conviction by formulating the FREPR even when the legislature is unable to domesticate international law.⁸⁵⁰

Nigeria has a dualist mode of domestication of treaties and the process requires several administrative processes before being presented to the National Assembly.⁸⁵¹ The procedure has been identified by the National Assembly as the reason for the delay in the domestication of treaties.⁸⁵² The preamble of the FREPR indicates a willingness on the part of the judiciary to adjudicate fundamental rights cases with more consideration of international law in spite of the legislature’s procedural problems.⁸⁵³ However, these statements in the preamble, although aspirational, do not form part of the law and so carry little weight.⁸⁵⁴

4.4.1 Horizontal application of the Bill of Rights

The 1999 Nigerian Constitution, unlike the South African Constitution does not expressly provide for a horizontal application of the Bill of Rights.⁸⁵⁵ However, section 1(1) of the 1999 Nigerian Constitution provides that:

⁸⁴⁹ *Okafor v Ntoka* (2017) LPELR-42794 (CA) 20.

⁸⁵⁰ Sanni 2011 11 *AHRLJ* 514.

⁸⁵¹ S.12(1) of the 1999 Nigerian Constitution.

⁸⁵² Ugochukwu 2014 1 *Transnational Human Rights Review (THRR)* 9; Abdulrauf “The Challenges for the Rule of Law Posed by the Increasing Use of Electronic Surveillance in Sub-Saharan Africa” 2018 18 *African Human Rights Law Journal* 386.

⁸⁵³ Fundamental Rights (Enforcement Procedure) Rules, 2009.

⁸⁵⁴ Sanni 2011 11 *AHRLJ* 525.

⁸⁵⁵ *Onwo v Oko* (1996) 6 NWLR (Pt. 456) 603: “It seems clear to me that in the absence of a clear positive prohibition which prohibits an individual to assert a violation or invasion of his fundamental rights against another individual, a victim of such invasion can also maintain a similar action in a court of law against another individual for his act that had occasioned wrong or damage to him or his property in the same way as an action he could maintain against the State for a similar infraction”; *Uzoukwu v Ezeonu II* (1991) 6 NWLR (Pt 200) 708; *Okoi v Inah* 1998(1) FHCLR 677.

"This Constitution is supreme and its provision shall have binding force on the authorities and persons throughout the Federal Republic of Nigeria."

The Bill of Rights, being a part of the Constitution, is binding on both authorities (vertically) and persons (horizontally). Section 1(1) of the 1999 Nigerian Constitution signifies an intention that the Bill of Rights should apply horizontally but this a controversial topic.⁸⁵⁶ The prevalent view of the Court has, however, been in favour of horizontal application of the Bill of Rights.⁸⁵⁷

In addition, section 46(1) of the 1999 Nigerian Constitution provides that persons can seek redress for an alleged infringement of their rights. There is no specification that redress can only be sought against the State. Judicial precedent indicates that the courts have held non-state actors liable for infringements of fundamental rights.⁸⁵⁸ For example, the Court of Appeal in *Eneye v MTN Nigeria Communications Ltd*⁸⁵⁹ held MTN liable for breach of the appellant's right to privacy.

Furthermore, in *Emerging Markets Telecommunications Services Limited (EMTS) v Eneye*,⁸⁶⁰ both the Federal High Court and Court of Appeal found that Emerging Markets Telecommunications Services Ltd infringed the right to privacy by sending unsolicited messages to the plaintiff/respondent. Mr. Eneye also sued MTN Nigeria for the unauthorised disclosure of his mobile phone number to unknown third parties who then continuously sent him unsolicited text messages.⁸⁶¹ The Court of Appeal held MTN liable for violations of Mr. Eneye's constitutional right to privacy and awarded damages of N5, 000, 000 (five million naira).

⁸⁵⁶ Nwauche "The Right to Privacy in Nigeria" 2007 1 *CALS Review of Nigerian Law and Practice* 88; *Aderinto v Omojola* 1998(1) FHCLR 101; *Ale v Obasanjo* (1996) 6 NWLR (Pt. 459) 384 (right to privacy); *Anigboro v Sea Trucks Ltd* (1995) 6 NWLR (Pt. 399) 35 (Freedom of Association); *Aniekwe v Okereke* (1996) 6 NWLR (Pt. 452) 61; *Agbai v Okagbue* (1991) 7 NWLR (Pt. 204) 391(Right to Property); *Salubi v Nwariaku* (1997) 5 NWLR (Pt. 505) 442 (freedom from discrimination).

⁸⁵⁷ *Emerging Markets Telecommunications Services Limited v Eneye* (2018) LPELR-46193 (CA) 25-29.

⁸⁵⁸ S.46(1) of the 1999 Nigerian Constitution provides as follows: "[a]ny person who alleges that any of the provisions of this Chapter (Chapter IV) has been, is being or likely to be contravened in any State in relation to him may apply to a High Court in that State for redress."

⁸⁵⁹ Appeal No: CA/A/689/2013 (unreported); The Federal High Court in *Anene v Airtel Nigeria Ltd*, Suit No: FCT/HC/CV/545/2015 (unreported) reached the same verdict and also awarded the claimant damages of N5, 0000 to the respondent.

⁸⁶⁰ (2018) LPELR-56193 (CA) 25-29.

⁸⁶¹ *Eneye v MTN Nigeria Communications Ltd*, Appeal No: CA/A/689/2013 (unreported); The Federal High Court in *Anene v Airtel Nigeria Ltd*, Suit No: FCT/HC/CV/545/2015 (unreported) reached the same verdict and also awarded the claimant damages of N5, 000, 000 to the respondent.

Furthermore, the Court of Appeal in *Igwe v Ezeanochie*⁸⁶² held the respondent liable for an infringement of the appellant's constitutional rights to freedom of movement, dignity of his person and liberty. The respondents were constantly harassing, intimidating, threatening, oppressing and detaining the appellants in police custody for their refusal to pay a residents' association levy. The act of detaining the appellants was that of the police, who should have been held liable for the infringement of the appellants' fundamental rights in this suit. Nonetheless, the suit indicates that non-state parties can be held liable for infringement of fundamental rights.

The decisions above have shown that courts interpret the Bill of Rights as applying horizontally. However, some authors have indicated that some courts still refuse to apply the Bill of Rights horizontally.⁸⁶³ It is submitted that an express constitutional provision on the horizontality of the Bill of Rights will provide clarity on the matter. The horizontal application of the Bill of Rights will instil certainty into the Nigerian legal framework, which may deter natural and juristic persons from infringing the human rights of others, as they could be held liable. Communications Service Providers can, therefore, be held liable for infringement of the right to privacy that could arise as a result of their participation in the unlawful execution of communications surveillance.

4.4.2 Enforcement of the Bill of Rights

In Nigeria, a person whose right to privacy or any other right has been infringed can seek redress in the court through the Fundamental Rights Enforcement Procedure. Section 46(1) of the 1999 Nigerian Constitution also provides that anyone whose fundamental right "has been, is being or likely to be contravened" can seek redress through a High Court of the State.⁸⁶⁴ The FREPR is subordinate legislation and cannot seek to domesticate international treaties. The ACHPR has been domesticated but the ICCPR and other international human rights treaties that Nigeria has ratified has not been domesticated.

The ACHPR should have been the only human rights treaty recognised by the FREPR. The preamble to the FREPR, even though commendable, cannot allocate powers to the High Court in excess of the 1999 Nigerian Constitution and other statutes. In spite

⁸⁶² (2009) LPELR-11885 (CA) 42.

⁸⁶³ Nwauche 2007 1 *CALS Review of Nigerian Law and Practice* 88; *Aderinto v Omojola* 1998 (1) FHCLR 101; *Ale v Obasanjo* (1996) 6 NWLR (Pt. 459) 384.

⁸⁶⁴ Order 2 of the FREPR.

of the problems with FREPR, it is the law through which fundamental rights are enforced in Nigeria. It can, therefore, be utilised to persuade courts to approach the interpretation of the Bill of Rights in a manner that aligns with the UDHR, ICCPR, ICESCR and even the decisions of the UN Human Rights Committee (HRC). This will be utilised to make recommendations in the next chapter.

4.5 Constitutional protection of the right to privacy

As stated in the previous chapters, the right to privacy is the primary right affected by the utilisation of communications surveillance. Section 37 of the 1999 Nigerian Constitution provides as follows:

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

Section 37 of the 1999 Nigerian Constitution specifically identifies communications of Nigerian citizens as protected by the right to privacy thereby protecting correspondence, telephone conversations and telegraphic communications.⁸⁶⁵ The specific mention of telegraphic conversations in the 1999 Nigerian Constitution indicates that the drafters of section 37 were not abreast of technological advancement, which had made telegraphs obsolete before the coming into effect of the 1999 Nigerian Constitution. Section 37 of the 1999 Nigerian Constitution is indicative of the earlier submission that the Bill of Rights was not the focus of the several constitutional amendments in Nigeria. In fact, the wording of the constitutional protection of the right to privacy has remained unchanged since the 1979 Constitution, despite the fact that there have been three alterations to the 1999 Nigerian Constitution.⁸⁶⁶

It is clear that the protection of the communication of citizens, whether electronic or not, is specifically mentioned in section 37. However, the activities mentioned in section 37 are not exhaustive and include data privacy. Even though metadata, as defined in chapter one, is not correspondence, conversations or communications, it is still provided for under the general umbrella of the “privacy of citizens”, which has been interpreted broadly by the court.⁸⁶⁷

⁸⁶⁵ *Nwali v Ebonyi State Independent Electoral Commission* 28.

⁸⁶⁶ The Constitution of the Federal Republic of Nigeria, 1979 https://constitutionnet.org/sites/default/files/nig_const_79.pdf (accessed on 2021-02-15).

⁸⁶⁷ *Nwali v Ebonyi State Independent Electoral Commission* 29.

The Court of Appeal in *Nwali v Ebonyi State Independent Electoral Commission* interprets the privacy of citizens as protection that embodies every aspect of a human being including:

“his body, his life, his person, his thought, conscience, belief, decisions, (including his plans and choices), desires, his health, his relationships, character, possessions, family etc”.⁸⁶⁸

The Court interpreted section 37 of the 1999 Nigerian Constitution as having a non-exhaustive capacity to accommodate new inventions in technologies or new protections of privacy that may arise from time to time. The activities protected by section 37 are, therefore, broad in ambit.

The Supreme Court in *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo* interpreted the right to privacy of a citizen as:

“[A] right to protect one’s thought, conscience or religious belief and practice from coercive and unjustified intrusion and one’s body from unwarranted invasion”.⁸⁶⁹

The Supreme Court in this suit defined the ambit of the right to privacy more clearly, stating that it is the right to be protected from coercive and unjustified intrusion and unwarranted invasion.⁸⁷⁰ This means that unlawful communications surveillance occurs when it is coercive, unjustifiable and unwarranted. The Supreme Court’s interpretation of the right to privacy reflects section 45 of the 1999 Nigerian Constitution that provides for the limitation of the right to privacy and other rights. Restrictions on rights are permissible under the Constitution when they are “reasonably justifiable in a democratic society”. Thus, a coercive and an unwarranted measure on the right to privacy is prohibited. The next section discusses the constitutional limitation of rights.

4.6 Limitation of constitutional rights

The legality of communications surveillance is determined by the interpretation of the terms in section 45 of the 1999 Nigerian Constitution. Section 45(1) of the 1999 Nigerian Constitution provides as follows:

“1 Nothing in sections 37 [right to private and family life], 38 [right to freedom of thought, conscience and religion], 39 [right to freedom of expression and the press], 40 [right to peaceful assembly and association] and 41 [right to freedom of movement] of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society

⁸⁶⁸ *Nwali v Ebonyi State Independent Electoral Commission* 35.

⁸⁶⁹ (2001) LPELR-1856 (SC) 10.

⁸⁷⁰ *Ibid.*

- 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 freedom of other persons.”

The limitation clause in section 45(1) applies to specific rights and does not relate to the other rights in sections 33-36 and 42-43.⁸⁷¹ Although many scholars refer to the provisions of section 45(1) of the 1999 Nigerian Constitution as the general limitation clause, there is no generality to the limitation clause in section 45(1) as it relates only to sections 37-41.⁸⁷²

There are three criteria that must be met by the party asserting their utilisation of section 45(1). First, the action restricting the rights must be backed by law. Secondly, the law must be “reasonably justifiable in a democratic society”. Thirdly, the action must be in the interest of defence, public health, public safety, public order, public morality or for the protection and freedom of other persons. Section 45(1) also provides that any action that limits the right to privacy and other rights mentioned in section 45(1) must be supported by law. Such law must also be reasonably justifiable and must be in the interest of defence, public safety, public health and, public morals, or in the interest of other persons.

The 1999 Nigerian Constitution does not provide definitions or factors for determining whether laws are reasonably justifiable. It furthermore does not define the terms “public health”, “public morals”, “public order”, “defence” and “public safety”. It is the duty of the courts to define these terms, a matter with which they struggle. The manner in which courts interpret section 45 determines whether the lawful utilisation of communications surveillance allows for arbitrariness. As discussed in chapter two, the HRC has indicated that communication surveillance is lawful and non-arbitrary if the domestic laws authorising it align with the purpose and object of the ICCPR.

Some of the activities of communications surveillance, such as interception of the content of communication and post-surveillance processing of data, are legally permissible in Nigeria.⁸⁷³ However, to ensure that communications surveillance is

⁸⁷¹ Ugochukwu 2014 *THRR* 628. Ss. 33 (right to life), 34 (right to dignity of human persons), 35 (right to personal liberty), 36 (right to fair hearing), 42 (right to freedom from discrimination), 43 (right to acquire property).

⁸⁷² Nwabueze *A Constitutional History of Nigeria* (1982) 118; Okonkwor “The Legal Basis of Freedom of Expression in Nigeria” 1978 8 *California Western International Law Journal* 265; Ugochukwu 2014 *THRR* 31.

⁸⁷³ Regulation 4 of the LICR.

utilised in a way that is non-arbitrary, section 45 of the 1999 Nigerian Constitution must be interpreted in a manner that advances fundamental rights and protects democracy.⁸⁷⁴ In *Olawoyin v Attorney General of Northern Nigeria*,⁸⁷⁵ the Supreme Court held that before a restriction upon a fundamental human right may be considered justifiable, it must be shown that the restriction is not “excessive or out of proportion to the object which it is sought to achieve”.⁸⁷⁶ The utilisation of communications surveillance by the State must therefore be proportional to the end pursued.

The next section attempts to identify these interpretative problems. The definitions of the terms utilised in section 45(1) are provided using case law and UN documents such as Siracusa Principles, the General Comments on the ICCPR and decisions of the UNHRC.

4.6.1 Any Law

The courts have applied a broad interpretation to the meaning of “any law” as provided in section 45(1) as including statutes, customary law, Islamic law and common law. The Court of Appeal in *Anzaku v Governor of Nassarawa State* posits that “[a]ny law is so encompassing an expression, though not limiting the type of law. It applies to any system, whether statute law, customary law, Islamic law or common law applicable in Nigeria”.⁸⁷⁷ It is also difficult to infer whether the law must be of general application as there is no indication of this. Rather, the 1999 Nigerian Constitution provides that “any

⁸⁷⁴ *IGP v ANPP* 38; *Klass v Germany*, App. No. 5029/71, (1978) pars [49-50]; *Leander v Sweden*, App. No. 9248/81, (1987), par [60]; *Camenzind v Switzerland*, App. No. 21353/93 (1997), par [45]; *Lambert v France* App. No. 46043/14, (2015) par [31]; Breyer “Telecoms data retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR” 2005 11 *European Law Journal* 371.

⁸⁷⁵ (1961) 1 *All Nigerian Law Report* (ANLR) 269; Dada “Judicial Remedies for Human Rights Violations in Nigeria: A Critical Appraisal” 2013 10 *Journal of Law, Policy and Globalisation* 1.

⁸⁷⁶ *Olawoyin v Attorney General of Northern Nigeria* 1 ANLR 324.

⁸⁷⁷ (2006) All FWLR (Pt. 303) 340-341; Nwauche “Law, Religion and Human Rights” 2008 8 *African Journal of Human Rights* 572; The term “any law” leaves a state of confusion in which it is unascertainable whether Islamic law and customary law can be the basis upon which the right to religion and conscience (section 38) is limited. The Shari’a Court of Appeal in *Safiyatu v Attorney-General of Sokoto State* (unreported judgement of the Sokoto State Shari’a Court of Appeal dated 25 March 2002) in upholding the appeal of a woman who was sentenced to death by stoning under the Shari’a law stated that “a written law” used in section 36(6) of the 1999 constitution means laws enacted in federal and state legislative houses and their subsidiary legislations as follows “a person shall not be convicted of a criminal offence unless that offence is defined and the penalty therefore is prescribed in a written law, and in this subsection; a written law refers to an Act of the National Assembly or a law of a state, any subsidiary legislation or instrument under the provisions of a law”. This indicates that there are conflicting interpretations of section 45(1) of the 1999 Constitution.

law” that is reasonably justifiable and which fulfils the provisions in section 45(1)(a) and (b), may limit the right to privacy.

The phrase “any law” is broad enough to cover subordinate legislation limiting rights, whether such legislation is of general application or not. This is problematic because the procedure for the formulation and bringing into effect of subordinate legislation in Nigeria is not uniform, unless the enacting law provides specific guidance.⁸⁷⁸ The result is that there is no mandatory provision permitting public commentary and scrutiny in relation to subordinate laws before they come into effect. This may seem innocuous, yet subordinate laws have the same force of law as an Act of Parliament or a Law of the House of Assembly and are binding on the people.⁸⁷⁹

In addition, the discussion in section 8 below indicates the problems that arise when subordinate legislation is the kind of law that limits fundamental rights. One such problem is that subordinate legislation, like the LICR, has the potential to overreach its ambit and attributes more power to the State to restrict rights. This is one of the reasons why the Siracusa Principles’ definition of “prescribed by law” is that the law must be of general application that is consistent with the ICCPR.⁸⁸⁰ Even though the LICR is of general application in terms of its applicability throughout the country, its ambit is limited to electronic communications. It is also not precise enough as required by the ICCPR, regarding what constitutes unlawful interception of communication. It therefore fails to align with the definition of “prescribed by law” in the Siracusa Principles.

Another issue arising from the phrase “any law” is the constitutional definition of a law in section 318 of the 1999 Nigerian Constitution. Sections 4 and 318 define law as “a law enacted by the House of Assembly of a State.”⁸⁸¹ It is trite that where a law defines

⁸⁷⁸ For example, Australia has a Legislative Instrument Act 2003. Similarly, the UK has the Statutory Instruments Act, 1946; See Benson *Delegated Legislation in Nigeria: The Challenges of Control* (2014) LLM in Advanced Legislative Studies, Institute of Advanced Legal Studies, School of Advanced Study, University of London 14; Olewo *Administrative Law in Nigeria* (1997) 66.

⁸⁷⁹ “It is trite that subsidiary legislation generally has the force of law” *Omatseye v Federal Republic of Nigeria* (2017) LPELR – 3871 (CA) 19-20 *Amusa v The State* (2003) LPELR-474 (SC).

⁸⁸⁰ Siracusa Principles, par [15] 7.

⁸⁸¹ House of Assemblies in Nigeria is the legislature of federating states in Nigeria. The enactments of the Federal legislature; the Senate and the House of Representatives, are defined in section 318 of the 1999 Nigerian Constitution as defined as an “Act”. Ezeanokwasa, Ewulum, Mbanugo “Religious Freedom and its Limitation Under the 1999 Constitution of Nigeria” 2016 7 *Nnamdi Azikwe University Journal of International Law and Jurisprudence* 63.

a word, the meaning ascribed to it must be adhered to.⁸⁸² The courts have mostly considered Acts of the National Assembly as the practical interpretation of the term “any law” capable of limiting the rights in the Bill of Rights. Nonetheless, it cannot be ignored that the interpretation of the term “law” in section 45(1) by the courts conflicts with sections 4 and 318. The definition of “any law” in section 45(1) is, therefore, confusing and does not provide clarity as prescribed by the ICCPR to constitute a law that can limit rights and curtail arbitrariness.

4.6.2 Reasonably justifiable in a democratic society

The definition of the phrase ‘reasonably justifiable’ is important because communications surveillance is a limitation primarily to the right to privacy. The safeguards available during the utilisation of communications surveillance depends on whether the constitutional limitation clause is interpreted in a manner that advances fundamental rights or not. The definition of whether a law is reasonably justifiable will determine the extent of the powers of the State in utilising communications surveillance.⁸⁸³ As discussed in chapter two, the ECtHR has stated that if the power to limit rights is too broad then the possibility of abuse is very high.⁸⁸⁴ This is an issue that may be of concern for Nigeria.

As mentioned before, the 1999 Nigerian Constitution inherited its Bill of Rights from previous Constitutions. Sections 37 to 40 of the 1960 Constitution were originally derived from articles 8 to 11 of the European Convention, which itself derived its Bill of Rights from the UDHR.⁸⁸⁵ However, section 45 of the 1999 Nigerian Constitution was modified to substitute the term “necessary” with “reasonably justifiable”.⁸⁸⁶ This provides a less restrictive interpretation of the limitation because “necessary” according to the Siracusa Principles and as seen in the South African Interim Constitution provides a higher standard of scrutiny for the limitation.⁸⁸⁷ The South African Constitution also utilises “reasonable and justifiable” instead of “necessary”

⁸⁸² *Nosiru Attah v The State* (1993) LPELR-598(SC).

⁸⁸³ Taiwo “The Legal Subject in Modern African Law: A Nigerian Report” 2006 7 *Human Rights Law Review* 24.

⁸⁸⁴ *Camenzind v Switzerland*, App. No. 21353/93 (1997), par [45]; *Lambert v France* par [31]; *Amann v Switzerland*, App. No.27798/95, (2000) par [76]; *Zakharov v Russia*, App. No. 47143/06, (2015) par [233].

⁸⁸⁵ Ugochukwu 2014 *THRR* 40.

⁸⁸⁶ Ugochukwu 2014 *THRR* 34.

⁸⁸⁷ *Ibid*; S.33(b)(bb) of 200 of 1993; Siracusa Principles, par [10] 6.

albeit with guiding factors.⁸⁸⁸ As discussed in chapter three, the guidelines in section 36(1)(a)-(e) of the Constitution provide the South African courts with clarity and objectivity in evaluating whether laws are reasonable and justifiable.⁸⁸⁹

Courts in several cases have incorrectly presumed that section 45(1) of the 1999 Nigerian Constitution is a provision that permits any law to invalidate the rights in sections 37-41. This is in part a result of the provision in section 45(1) that states, “[n]othing shall invalidate any law...” A correct interpretation of section 45(1) rebuts the presumption that laws limiting rights in section 45(1) are automatically constitutionally valid.⁸⁹⁰ The duty of the court is to evaluate whether the law seeking to limit rights is reasonably justifiable in a democratic society and is for, at least, one of the legitimate purposes listed in section 45(1)(a) & (b).⁸⁹¹ Section 45(1) must be interpreted in light of the underlying social, political and economic conditions of the society.⁸⁹²

The Court of Appeal in *Nwali v Ebonyi State Independent Electoral Commission*⁸⁹³ stated that a law that is reasonably justifiable is determined by:

“the purpose which a law intends or seeks to achieve or the mischief it seeks to avoid together with the existing factual situation that prompted its making...”

The Supreme Court in *Williams v Majekodunmi*⁸⁹⁴ in interpreting “reasonably justifiable in a democratic society” stated:

“Those words... must be read in the context of the Constitution, and more particularly in the context of Chapter III in which they occur. The Chapter confers certain fundamental rights which are regarded as essential and which are to be maintained and preserved; and they are to serve as a norm of legislation under majority rule, which is the form or rule pervading the constitutions. If they are to be

⁸⁸⁸ 1995 (3) SA 391 par [104]; S.36(1)(a)-(e) of the Constitution; Rautenbach 2014 17 “Proportionality and the Limitation Clauses of the South African Bill of Rights” *Potchefstroom Electronic Law Journal PELJ* 2240.

⁸⁸⁹ Currie and De Waal *The Bill of Rights Handbook* 150.

⁸⁹⁰ Nwabueze *Constitutional History* 118.

⁸⁹¹ *Nwali v Ebonyi State Independent Electoral Commission* 53-54; Nwabueze *Constitutional History* 118; Okonkwo, “The Legal Basis of Freedom of Expression in Nigeria” 1978 *California Western International Law Journal* 86; Robert-Wray “Human Rights in the Commonwealth” 1968 17 *International and Comparative Law Quarterly* 908; Taiwo “The Legal Subject in Modern African Law: A Nigerian Report” 2006 7 *Human Rights Review* 24; Alexy “The Construction of Constitutional Rights” 2010 4 *Law and Ethics Human Rights* 20.

⁸⁹² *Nwali v Ebonyi State Independent Electoral Commission* 64.

⁸⁹³ *Nwali v Ebonyi State Independent Electoral Commission* 50.

⁸⁹⁴ [1962] 1 All Nigerian Law Report 413.

invaded at all, it must be only to the extent that is essential for the sake of some recognised public interest, and may not farther.”⁸⁹⁵

Even though the Supreme Court made a statement on the importance of evaluating statutes in light of the Bill of Rights, there was no development of guidelines for determining whether statutes limiting rights are reasonably justifiable in a democratic society.⁸⁹⁶ Instead, a subsequent decision in *Asari-Dokubo v Federal Republic of Nigeria*⁸⁹⁷ lacked an evaluation of whether the law is reasonably justifiable. In this case, the Supreme Court declared that the protection of national security takes priority over the protection of human rights in all cases.

The Court of Appeal in *Federal Republic of Nigeria v Daniel*⁸⁹⁸ held that section 41 of the National Drug Law Enforcement Agency Act (NDLEA Act) that provides for a warrantless search by the NDLEA is reasonably justifiable in the interest of public safety and public health, as section 45(1) is “unequivocally far-reaching”.⁸⁹⁹ The Court did not analyse whether the NDLEA Act was reasonably justifiable. Instead, the Court reached its decision based on the fact that a statute exists that limits the right in section 45(1). Again, the Court’s decision was based on the broad provision that “nothing shall invalidate any law”.⁹⁰⁰ This was unfortunate as the Court of Appeal lost an opportunity to provide guidelines for determining whether a law is reasonably justifiable.

⁸⁹⁵ At 426; see also, *Chukwuma v Commissioner of Police* [2005] 8 NWLR (Pt. 927) 278; *Inspector General of Police v All Nigeria Peoples Party* 20.

⁸⁹⁶ Also, in *Osawe v Registrar of Trade Unions*, (1962) NWLR (Pt. 927) 278, the Supreme Court held the registration of trade unions under the Trade Unions Act 1986 as constitutionally justified under the 1979 Constitution which had a similar limitation clause with section 45 of the 1999 Nigerian Constitution. However, it still did not develop a guideline for determining whether a statute is reasonably justifiable.

⁸⁹⁷ (2007) LPELR-958 (SC) 36.

⁸⁹⁸ (2011) LPELR-4152 (CA).

⁸⁹⁹ S. 41(1) of the National Drug Law Enforcement Agency Act CAP.N30, LFN 2004 provides that “any police officer, customs officer, or National Drug Law Enforcement Agency officer involved in the enforcement of the provisions of the Act may –

(i) Without warrant, enter and search any land, building or carrier, including aircraft, vehicle or container or any other instrumentalities whatsoever which he has reason to believe is connected with the commission of an offence under this Act;

(ii) May perform, test and take samples of any substance relating to the commission of an offence which are found on the land, building or carrier, including aircraft, vehicle, container or any other instrumentalities whatsoever searched pursuant to paragraph (a) of this subsection;

(iii) Arrest any person whom he has reason to believe has committed an offence under this Act;

(iv) Seize any item or substance which he has reason to believe has been used in the commission of an offence under this Act.”

Federal Republic of Nigeria (FRN) v Daniel, (2011) LPELR-4152 (CA)18; Dada 2012 IJHSS 42; *Director of State Security Services v Agbakoba* (1999) 3 SCNJ 1; *Solarin v IGP* (1983) 1 FNLR 415; *Shugaba Darman v Minister of International Affairs* (1980) FNL 203.

⁹⁰⁰ Nwabueze, *A Constitutional History of Nigeria* (1982)118.

The Court of Appeal should have analysed whether the NDLEA Act is reasonably justifiable. Only after arriving at a positive conclusion that the statute is reasonably justifiable can the court determine whether the limitation of the right in the circumstances is proportional to the legitimate aim pursued. It is, therefore, submitted that section 45(1) of the 1999 Nigerian Constitution is only as far-reaching as an accurate interpretation of “reasonably justifiable” permits.

Also, the Court of Appeal in *Hassan v Economic and Financial Crimes Commission* (EFCC) stated that section 45(1) has watered down the effect of section 37 of the 1999 Nigerian Constitution.⁹⁰¹ While it is true that the sentence “nothing in sections 37... shall invalidate any law” is too broad, the watering down of sections 37- 41 is mostly a result of the courts’ refusal to evaluate the validity of laws in light of whether they are reasonably justifiable.

Justice Abiru, concurring with the lead judgment in *Hassan v EFCC*, stated that section 27 of the Police Act that provides for arrest without warrant is reasonably justifiable. He further stated that:

“it is clear that where it is shown that the Police acted reasonably within its powers under the Police Act in the investigation of a criminal complaint and with reasonable grounds to believe that a person had committed a criminal offence or is likely to commit one, the necessary curtailment of the fundamental rights...cannot amount to a breach of that person’s fundamental rights”.⁹⁰²

The Court of Appeal in this suit interpreted section 45 (1) of the 1999 Nigerian Constitution as validating the mere existence of a statute for the limitation of fundamental rights. The court should have evaluated whether the provisions of the Police Act were reasonably justifiable in a democratic society.

Many court decisions interpreted the existence of a statute limiting rights as constitutionally valid. However, the Court of Appeal in *Inspector General of Police v All Nigeria Peoples Party (IGP v ANPP)*⁹⁰³ deviated from this approach. The Court in this case held that the provision of section 1(1)(2)(3)(4)(5) and (6) of the Public Order Act (POA) which requires a license for public assemblies, meetings, processions organised on a public road or place of public resort, is not reasonably justifiable in a

⁹⁰¹ (2013) LPELR-22595 (CA)10.

⁹⁰² *Hassan v EFCC*, 40.

⁹⁰³ (2007) LPELR-8217 (CA) 1.

democratic society.⁹⁰⁴ The Court further stated that the POA “leaves unfettered the discretion on the whims of certain officials, including the police.”⁹⁰⁵

The Court held that the right of citizens to assemble freely and associate with others includes the right to hold rallies or processions or demonstrations. The provisions of the POA stifle these rights rather than preserve them and it is, therefore, an “aberration to a democratic society”. In addition, the Court utilised the qualities of a democratic society as provided for in section 14(1) and (2) of the 1999 Nigerian Constitution and as exhibited by comparable civilised democracies to conclude that the above stated provisions of the POA are not reasonably justifiable.⁹⁰⁶

Two guidelines can be inferred from this: firstly, the norm of other comparable democratic societies can be an indication as to whether a statutory provision is reasonably justifiable in a democratic society. Secondly, the State, having unfettered discretionary power allocated to it by statute, can be a determinant on whether the law is reasonably justifiable. The Court of Appeal further stated that:

“Even though the Governments [*sic*] purpose may be legitimate and substantial that purpose cannot be pursued by means that broadly stifle fundamental personal liberties”⁹⁰⁷

The Court of Appeal did not expressly provide guidelines for determining reasonableness and justifiability, however it put more effort than in earlier judgments to analyse the constitutional validity of the POA in terms of section 45 of the 1999 Constitution. The constitutional validation analysis, therefore, involves the court analysing whether the statute limiting the right is reasonably justifiable and thereafter verifying the purpose of such limitation.⁹⁰⁸

⁹⁰⁴ *IGP v ANPP* 43; Nwauche 2008 8 *AJHR* 587.

⁹⁰⁵ *IGP v ANPP* 30.

⁹⁰⁶ *IGP v ANPP* 29, 30,37,44. “I must explain at this stage that a document such as the Nigerian Constitution, which is written, cannot be interpreted following judicial decisions based on principles of common law or judicial decisions that interpreted Statutes or Constitutions which are not in materia with the provisions of the [C]onstitution. However judicial decisions based on foreign Statutes and Constitutions with similar or identical provisions as the Nigerian Constitution carry some measure of weight and persuasive effect, but they lack binding effect on Nigerian principle of stare decisis.” *Nigerian Port Authority v Akar* 1965 (1) All NLR 526; *Obadara v President Ibadan West District Council Grade B Customary Court* (1964) 1 All NLR 336; *Alhi v Okulaja*1(972) 2 All NLR 351; *A.G Ondo State v A.G Federation* (2002) 9 WLR (Pt. 772) 222; *Olafisoye v Federal Republic of Nigeria* (2004) 4 NWLR (Pt. 804) 580; *Adigun v A.G Oyo State* (No. 2) 1987 2 NWLR (Pt. 56) 197.

⁹⁰⁷ *IGP v ANPP* 42.

⁹⁰⁸ International Institute for Democracy and Electoral Assistance “Limitation Clauses” (November 2014) https://constitutionnet.org/sites/default/files/limitations_clauses.pdf (accessed 2021-02-01) 14.

The Interim Constitution of South Africa had similar problems as discussed in chapter three.⁹⁰⁹ The Constitution of South Africa, in providing express guidelines, creates a procedure for the enquiry into the constitutional validity of statutes. This procedure, as discussed in chapter three, commences with the determination of the scope of the right limited as provided by section 36(1)(a) of the Constitution.⁹¹⁰ Thereafter, the court evaluates whether statutes are reasonable and justifiable based on the guidelines provided in section 36(1)(a)-(e) of the Constitution. As a result, South African courts cannot ignore the objective analysis that the constitutional validity of statutes requires.⁹¹¹

4.6.3 Legitimate aims for limiting constitutional rights in the 1999 Nigerian Constitution

The 1999 Nigerian Constitution does not provide for definitions of these terms. The Siracusa Principles document has, however, provided extensive explanations for these terms. As stated in chapter two, the Siracusa Principles aim to define terms utilised in the limitation of rights in the ICCPR. While many judicial precedents on section 45(1) have utilised the legitimate purposes in section 45(1)(a) and (b) in the 1999 Nigerian Constitution as the reasons for justifying the limitation of rights affected by the provision, there has not been any judgment defining these terms in the Nigerian context.⁹¹²

The reason for the reliance on the definition in the Siracusa Principles here is because the HRC has also relied on these terms to reach decisions that require interpretation of the terms addressed in the Siracusa Principles. It is also a very instructive document for Nigeria because two of the experts involved in the compilation of this document are

⁹⁰⁹ As mentioned in Chapter 3, sec. 3.6, the Constitutional Court in *S v Makwanyane* laid down guiding principles for determining whether the provision of a statute or action is reasonable and justifiable. The guidelines were adopted into section 36(1)(a)-(e) of the Constitution and have assisted the courts in the interpretation of the phrase reasonable and justifiable in the limitation clause. Similar guidelines would assist the Nigerian courts when assessing the justifiability of a statute limiting rights.

⁹¹⁰ *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In Re Hyundai Motor Distributors (Pty) Ltd v Smit* par [18]; *National Coalition of Gay and Lesbian Equality v Minister of Home Affairs* par [59]; *Phillips v Director of Public Prosecution* (WLD) 2003 (4) BCLR 357 (CC) par [23]; *Qwelane v South African Human Rights Commission* 2020 (2) SA 124 (SCA) par [51]; *Minister of Justice and Constitutional Development v Prince* 2019 (1) SACR 14 (CC) pars [25-26].

⁹¹¹ *Amabhungane v Minister of Justice* 2020 (1) SA 90 (GP) pars [53, 68, 89]; *Case v Minister of Safety and Security*; *Curtis v Minister of Safety and Security* 1996 (1) SACR 587 (CC) pars [48-63]; *S v Manamela (Director-General of Justice Intervening)* 2000 (5) BCLR 491 (CC) par [96].

⁹¹² To the knowledge of this researcher.

well respected jurists (Justices Taslim Olawale Elias and Adetokunbo Ademola were both Chief Justice of Nigeria) thus indicating some Nigerian influence in the document.

Some statutes, for example the National Securities Act, have similar terms to those used in section 45(1). The definitions in these statutes can be used to provide definitions for the terms in section 45(1), albeit with caution as the court held in *IGP v ANPP* that judicial interpretation of statutes cannot be utilised to interpret the Constitution.⁹¹³ Nevertheless, judicial interpretation of other statutes by the courts is instructive in providing context to the terms in issue and such jurisprudence prevents the executive from overreaching.

Definitions of these terms in foreign jurisdictions are also utilised to provide context to the meaning of the terms in section 45(1) because as shown in chapters two and three and in *IGP v ANPP*, interpretations from comparable democracies are important and have persuasive value. As the world is a global village and since the 1999 Nigerian Constitution is arguably a living document, it ought to be interpreted in a manner that takes the current global positions on all issues into account.⁹¹⁴ For example, the decisions of the ECtHR are instructive in matters relating to communications surveillance. However, lessons derived from foreign jurisdictions must be contextualised to be relevant.⁹¹⁵

One of the interpretive principles in the Siracusa Principles is that the limitation of a right “shall not be interpreted so as to jeopardize the essence of the right concerned”.⁹¹⁶ This principle was one of the deciding factors for the Court of Appeal’s decision on the constitutional invalidity of the affected sections of the POA in *IGP v*

⁹¹³ *IGP v ANPP* 37.

⁹¹⁴ The 1999 Constitution being defined as a living document is contentious because the interpretation of “reasonably justifiable” restricts fundamental rights as if Nigeria is in an autocracy rather than a democracy. Many judicial decisions took the position of interpreting fundamental rights in a manner that supports the absolute power of the State to limit rights contrary to the current democratic reality of the country.

⁹¹⁵ Markesinis, O’Cinneide, Fedtke and Hunter-Henin “Concerns and Ideas about the Developing English Law of Privacy (and how Knowledge of Foreign Law might be of Help)” 2004 52 *The American Journal of Comparative Law (AJCL)* 202. The study of foreign law is rarely meant to lead to wholesale incorporation of foreign concepts, notions, and solutions but it can lead to new ideas infiltrating national law; it may also help dispel myths about threatened and imagined consequences in the event of a local change in the law”.

⁹¹⁶ Siracusa Principles Document, par [2] 6; Hynes “Online Privacy and Surveillance” in *The Social, Cultural and Environmental Costs of Hyper-Connectivity: Sleeping through Revolution* (2021) 87 “An individual’s freedom to protest when they feel something needs changing, to freely associate with others, to move around their own country without hindrance, to read and to write without wondering who is tracking their every movements and motives; these are all universally recognised fundamental rights in democratic societies”.

ANPP. Although, the Siracusa Principles were not quoted, the fundamental principles were the same.

4.6.3.1 Defence

Many international treaties and Bills of Rights utilise “national security” instead of “defence”. The word “defence” in section 45(1) is a narrower term that connotes military activities. The purpose of the ministry of defence and the definition of its activities is instrumental in defining “defence”. The National Security Agencies Act established three agencies to conduct matters relating to national security effectively.⁹¹⁷ These agencies are the Defence Intelligence Agency (DIA), the National Intelligence Agency (NIA) and the Department of State Security Service (DSS).⁹¹⁸ The DIA is responsible for matters relating to defence and is charged with the responsibility of managing matters relating to the military.⁹¹⁹ The NIA is responsible for security matters outside Nigeria (foreign intelligence) and “that are not related to military issues”.⁹²⁰ The DSS is in charge of matters concerning internal security and that are not of a military nature.⁹²¹

This classification of national security signifies that “defence” is only a branch of national security that relates to the activities of the military.⁹²² A strict interpretation of the definition of “defence” will mean that only matters relating to threats to national security of a military nature can limit fundamental rights in section 45(1) of the 1999 Nigerian Constitution. It is noted that the 1999 Nigerian Constitution is a document that must be interpreted broadly to give meaning to specific circumstances.⁹²³ However, this broad interpretation does not apply to the limitation clause as it can undermine human rights. Even if the Constitution is interpreted broadly, it should not lead to a substitution of terms. Hence, utilising the term “national security” rather than “defence” provides a different interpretation from the Constitution.

⁹¹⁷ S.1 of the National Security Agencies Act of 1986.

⁹¹⁸ *Ibid.*

⁹¹⁹ S.2(1) of the National Security Agency Act.

⁹²⁰ S.2(2)(a) – (c) of the National Security Agency Act.

⁹²¹ S.2(3) of the National Security Agency Act.

⁹²² *IGP v ANPP*, 39; *Awolowo v Shagari* (1979) 69 SC 51; *Alamiyeseigha v FRN* (2006) 16 NWLR (Pt. 1004) 1; *Rabiu V State* (1960) 8 SC 130; *A.G Bendel State v A.G Federation* (1981) 10 SC 1; *Owena v Nigerian Stock Exchange Ltd* (1997) 8 NWLR Pt. 515; *Bronik Motors Ltd v Wema Bank Ltd* (1983) 1 SCNLR 296.

⁹²³ *Ibid.*

The Supreme Court in *Asari-Dokubo v Federal Government of Nigeria* held that “where National Security is threatened...human rights or the individual right of those responsible take second place”.⁹²⁴ The Court uses “national security” rather than “defence” as one of the legitimate aims for restricting rights. The Court erred in substituting “national security” for “defence”. The Court did not define “national security” but held that the appellant’s action involves “creating a situation where the government of the Federal Republic of Nigeria could yield to force or expose the public to serious danger”.⁹²⁵ This description is too vague especially for describing a circumstance that can potentially lead to suspension of human rights.

The decision of the Supreme Court has given rise to the misconception on the part of the executive that human rights must be suspended once any threat to national security is invoked. The current Nigerian President, Rtd. Major-General Muhammadu Buhari has stated that the rule of law is subject to national security and the public interest.⁹²⁶ This misconception of the role of the rule of law in a democracy has led to many executive actions that restrict human rights unjustifiably.⁹²⁷ Section 45(1) provides for the limitation of human rights not their suspension. Since the practice of the Nigerian courts is to limit rights for the protection of national security, the definition of national security should be provided in the context of international law.

The Siracusa Principles have narrowed the definition of national security by providing circumstances when it can and cannot be employed. The term “national security” can be utilised as a legitimate aim to limit constitutional rights where there are threats to the “existence of the nation or its territorial integrity or political independence against force or threat of force.”⁹²⁸ “National security” cannot be utilised to limit rights in order to “prevent merely local or relatively isolated threats to law and order”.⁹²⁹ The Siracusa

⁹²⁴ (2007) LPELR-958 (SC) 36.

⁹²⁵ *Asari-Dokubo v Federal Republic of Nigeria* 29-30.

⁹²⁶ Ishiekwene “Lawyers, Buhari and the Ruins of Law” (31 August 2018) *Vanguard News* <https://www.vanguardngr.com/2018/08/lawyers-buhari-and-the-ruie-of-law/> (accessed 2021-08-06).

⁹²⁷ *Ibid.* The President Muhammadu Buhari on 6 June 2021 announced the suspension of the use of Twitter in Nigeria stating national security as the purpose of the ban. In 2018, the former Inspector General of Police, Ibrahim Idris harassed and attacked some editorial staffs of Premium Times. He also detained and froze the account of one Samuel Ogundipe who was one of the editorial staffs of Premium Times (an on-line news agency) for threatening national security because they allegedly leaked his memo to the Vice-President. Igwe “The Rule of Law and National Security in Nigerian Democracy: A Contemporary Issue under the Aegis of International Law” 2021 7 *Athens Journal of Law* 154-155.

⁹²⁸ Siracusa Principles, pars [27-32] 8-9.

⁹²⁹ *Ibid.*

Principles also state that the “systematic violation of human rights” by the State is on its own, a threat to national security, international peace and security.⁹³⁰ The State should not use the excuse of protecting national security to stifle opposition to human rights violations.⁹³¹

4.6.3.2 Public morals

The term “public morals” is one of the contentious terms in limitation clauses globally and is derived from the UDHR.⁹³² The phrase is particularly problematic in Nigeria, which criminalises same-sex marriage and/or association while also guaranteeing freedom of association, thoughts, opinion, religion and the right to privacy.⁹³³ The public polls conducted in Nigeria before the Same Sex Prohibition Act, 2013⁹³⁴ was enacted indicated that the majority of the public who were opposed to same-sex relations did so because of religious convictions and morals.⁹³⁵ Meanwhile, Nigeria is a Republic without a unified religion. The prohibition of same-sex relationships based on the justification of morality influenced by religion is, therefore, inconsistent with the 1999 Nigerian Constitution.⁹³⁶ The rights of the minority ought not to be denied in order to placate the majority.⁹³⁷

In General Comment No. 22 of the ICCPR, the HRC stated that public morals are not morals of a single religion:

“The Committee observes that the concept of morals derives from many social, philosophical and religious traditions; consequently, limitations on the freedom to

⁹³⁰ *Ibid.*

⁹³¹ *Kopp v Switzerland* App. No. 23224/94 (1998), par [64]; *Valenzuela Contreras v. Spain*, (1998), par [46]; *Malone v United Kingdom* App. No. 8691/79, (1984) par [67]; *Huvig* par [29]; *Weber and Saravia* App. no. 54934/00 (2006) pars [103-106]; *Bigbrother Watch* par [308]. “Therefore, to prevent ‘national security’ becoming a catch-all term that is used in ways that curtail or undermine democracy, the definition of what constitutes a genuine threat should be carefully and narrowly determined”. Ahmed and Bulmer “Limitation Clauses” *International IDEA (Institute for Democracy and Electoral Assistance) Constitution-Building Primer 11* 2ed (2017) 9.

⁹³² Article 29 of the Universal Declaration of Human Rights.

⁹³³ S.5(1) of the Same Sex Prohibition Act, 2013.

⁹³⁴ Same Sex Prohibition Act, 2013.

⁹³⁵ “Nigerians support Anti Same-sex Bill” (20 June 2013) <https://www.vanguardngr.com/2013/06/nigerians-support-an> (accessed 2021-01-27).

⁹³⁶ Nwauche “Law, Religion and Human Rights” 2008 8 *African Journal of Human Rights* 573. Nwauche argues that Nigeria is much more of a religious country than it admits to being.

⁹³⁷ Igwe “The Rule of Law and National Security in Nigerian Democracy: A Contemporary Issue under the Aegis of International Law” 2021 7 *Athens Journal of Law* 152.

manifest a religion or belief for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition.”⁹³⁸

The HRC noted further in General Comment No. 34 that “any such limitations must be understood in the light of universality of human rights and the principle of non-discrimination”.⁹³⁹ The Siracusa Principles further state that the concept of public morality evolves with time and use of public morals as a limitation of constitutional rights must uphold the principles of non-discrimination as defined in the ICCPR.⁹⁴⁰

Public morals also change from time to time as seen in the views of the HRC on same-sex relations in *Hertzberg v Finland*, 1982 and *Irina Fedotova v Russian Federation*, 2012.⁹⁴¹ In the former suit, the HRC permitted the prohibition of same sex relations based on public morals as justifiable.⁹⁴² However, in the latter suit, the HRC declared a Ryazan Regional law that provides punishment for same-sex relations using the argument of public morals as unjustifiable.⁹⁴³ Fundamental rights cannot, therefore, be limited based on public morals, without considering the changes in the society concerning that issue. It is important that the interpretation of public morals be reassessed in Nigeria so that communications surveillance will not be utilised to victimise persons in same-sex relationships. This is because currently same-sex relationship is a crime in Nigeria and a person can be subject to surveillance for offences under the Same-Sex Prohibition Act, 2013.

4.6.3.3 Public health

The limitation of rights as a result of public health must be utilised in a situation that demands the prevention of “disease or injury or providing care for sick people”.⁹⁴⁴ The health threat must also have the potential of constituting a serious threat to the health of the population or individual members of the population.⁹⁴⁵ For example, while using a facemask may reduce the spread of flu, imposing the compulsory use of face masks

⁹³⁸ UN Human Rights Committee (HRC), *CCPR General Comment No. 22: Article 18 (Freedom of Thought, Conscience or Religion)*, 30 July 1993, CCPR/C/21/Rev.1/Add.4, <https://www.refworld.org/docid/453883fb22.html> (accessed on 10 February 2021).

⁹³⁹ UN Human Rights Committee (HRC), General comment no. 34, Article 19, Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34 <https://www.refworld.org/docid/4ed34b562.html> (accessed 2021-02-10).

⁹⁴⁰ Siracusa Principles, par [27] 8-9.

⁹⁴¹ Communication No. 61/1979, 2 April 1982; Communication No. 1932/2010, 31 October 2012.

⁹⁴² *Ibid.*

⁹⁴³ *Ibid.*

⁹⁴⁴ Ahmed and Bulmer “Limitation Clauses” International IDEA (Institute for Democracy and Electoral Assistance) Constitution-Building Primer 11(2017) 2ed 9.

⁹⁴⁵ Siracusa Principles, par [25] 8.

to curtail a flu epidemic may be an overreach of the definition of protection of public health. On the other hand, imposing the use of a facemask to reduce infection of COVID-19 may be within the definition of prevention of serious threat to health and so a justifiable aim for a statute mandating the use of facemasks. Certain laws, for example, may prevent a health worker from wearing jewellery such as a crucifix and rings to prevent contamination of patients.⁹⁴⁶ The nature of the public health crisis will therefore determine the rights to be limited and the extent of the restriction under the law.

The COVID-19 pandemic has shown that the existence of a “public health” crisis does not require the absolute limitation of all rights. The public health crisis must be assessed to determine the rights that require limitation and the extent of such limitation. For example, as mentioned in Chapter three, South Africa tried unsuccessfully to use communications surveillance through location tracking to identify the proximity of phones to an infected person. There was, however, a successful balancing of the limitation of the right of privacy and the use of communications surveillance.⁹⁴⁷

4.6.3.4 Public order and public safety

Public order and public safety are both phrases that are often interpreted broadly and utilised by the State to limit rights arbitrarily, especially in relation to communications surveillance. This broad interpretation led to the POA being challenged in *IGP v ANPP* and some of its sections being declared unconstitutional. The respondents were unable to justify the purpose of a prior police scrutiny for protests, which they argued, was to prevent violence and breach of peace and which the Court held to be “highly speculative”.⁹⁴⁸ Section 315 of the 1999 Nigerian Constitution empowers the National Assembly to enact laws for public order and public safety.⁹⁴⁹ The analysis of laws limiting rights within the context of whether a limitation is reasonably justifiable or not will assist the court in determining the boundaries of the State in preserving public

⁹⁴⁶ Conway, Wu and Lipner “Guidance on Hand Jewelry for Prevention of COVID-19 Transmission in Healthcare” 2020 33 *Dermatologic Therapy* 1; Ward “Hand Adornment and Infection Control” 2007 16 *British Journal of Nursing* 654-656.

⁹⁴⁷ Chapter 3, sec.3.8.6.

⁹⁴⁸ *ANPP v IGP*, 40 and 43.

⁹⁴⁹ *Chukwuma v Commissioner of Police* (2005) 8 NWLR (Pt.927) 287.

order and public safety. Once a law is not reasonably justifiable, its purpose is irrelevant.

In addition, in *Nwankwo v The State*⁹⁵⁰ the Court of Appeal dispelled an attempt by the State to stifle the right to freedom of expression through the offence of sedition. The Court of Appeal overturned the decision of the lower court where the appellant was found guilty of publishing and distributing seditious materials.⁹⁵¹ Sedition is an offence that seeks to protect the government and as often argued by the State, is a way of maintaining public order.⁹⁵² The Court of Appeal held that the appellant was entitled to exercise his right to freedom of expression by publishing a book that criticised the government of Anambra State.⁹⁵³ The Court further stated that criticism is necessary for a healthy democracy and that the charge against the appellant was inconsistent with section 36 (right to freedom of expression and the press) of the 1979 Constitution.⁹⁵⁴ The preservation of “public order and public safety” is therefore a limitation of rights that must be balanced with the rights that it seeks to restrict. Again, a proportionality evaluation between rights and its limitations is necessary to determine whether a law is reasonably justifiable.

In assisting the balancing exercise, the definition of public safety by the Siracusa Principles can be utilised further to determine the boundaries of the State in preserving of public safety. The Siracusa Principles define public safety as “protection against danger to the safety of persons, to their life or physical integrity, or serious damage to property”.⁹⁵⁵ It further states that the limitation of rights for the sake of public safety must not be vague or arbitrary and it may only be invoked when there are existing adequate safeguards and effective remedies against abuse.⁹⁵⁶

⁹⁵⁰ (1985) 6 NCLR 228.

⁹⁵¹ Igwe and Alunegbe “The Law of Sedition in Contemporary Nigerian Criminal Law: A Review of the Case of *Arthur Nwankwo v The State*” (July 2018) https://www.researchgate.net/publication/326380881_The_Law_of_Sedition_in_Contemporary_Nigerian_Criminal_Law_A_Review_of_the_Case_of_Arthur_Nwankwo_v_The_State (accessed on 2021-03-01).

⁹⁵² Chima “Democracy in Danger: Law of Sedition and the Idea of Free Press” https://www.academia.edu/12981450/Democracy_in_danger_law_of_sedition_and_the_idea_of_a_free_press (accessed on 2021-03-01) 5.

⁹⁵³ *Nwankwo v The State* [1985] 6 NCLR 228.

⁹⁵⁴ *Ibid.*

⁹⁵⁵ Siracusa Principles Document, pars [33 & 34] 9.

⁹⁵⁶ *Ibid.*

When the preservation of public safety is the reason why communications surveillance is utilised, the law backing the action must be subject to judicial scrutiny as an oversight mechanism. It must also permit the surveillance subject to challenge such law and/or seek compensation for any unlawful surveillance.

4.6.3.5 For the purpose of protecting the rights and freedom of other persons

Considering the rights and freedom of others requires a balancing/proportionality exercise between rights. Unfortunately, there are not many cases which use a proportionality analysis in Nigerian law. Usually, courts merely balance the powers of the State to limit rights with the protection of the rights.⁹⁵⁷ The duty of the State regarding criminal justice procedure falls under the category of the limitation of rights for the purpose of protecting the rights and freedoms of others. The power of the State in this regard must be balanced with the nature of the right to be restricted and considering the aim pursued for such restriction. As there are many offences that the State will be required to investigate, some of which are minor offences, the extent of limitation of rights for minor offences will vary in comparison to serious offences like felonies.⁹⁵⁸

One of the key issues in communications surveillance is deciding the type of offences for which communications surveillance can be employed. International and regional laws have condemned any utilisation of communications surveillances for any offence other than a serious offence. This is because of the highly intrusive nature of communications surveillance on a person's privacy. Consequently, the nature of the right and the importance of the limitation and its purpose must be evaluated to determine the extent of limitation that is required in each circumstance.

4.6.4 The lack of objective interpretation of the legitimate aims

The legitimate aims for limiting rights in section 45(1)(a) and (b) must not be evaluated in a manner that best protects rights and this depends largely on how courts interpret the limitation of right that is reasonably justifiable. The majority of the legitimate aims in section 45(1)(a) & (b) have not been extensively assessed by the courts. This, as

⁹⁵⁷ Ugochukwu 2014 *THRR* 34.

⁹⁵⁸ S.6 of the Nigerian Criminal Code Act Cap C38 of the Laws of Federation of Nigeria 2004 provides for three categories of offences. They are simple offences, misdemeanours and felonies. Simple offences and misdemeanours are offences punishable with an imprisonment of less than six months or less than three years respectively. Felonies are punishable with an imprisonment of three years or more.

indicated above, is a result of the insufficient guidance afforded to the factors to be considered when limiting rights in terms of the 1999 Nigerian Constitution. Each judge has to decide, without any guideline from the 1999 Nigerian Constitution, whether a limitation is reasonably justifiable. Section 45(1)(a) & (b) which limits the right to privacy and other rights, therefore, lacks clarity, objective interpretation and constitutional guidance. The proposed reforms to these problems are addressed in chapter five.⁹⁵⁹

4.7 The common law and the right to privacy in Nigeria

The common law, along with the law of equity and the statutes of general application that were in force in England on the first day of January 1990, are received English laws retained by Nigeria after her independence from Britain in 1960.⁹⁶⁰ Although English judicial precedent does not form part of the received English law, it continues to have persuasive force in Nigerian Courts.⁹⁶¹ The law of torts forms part of the common law that “was developed by judges of the old common law courts out of the general customs and practices among the English communities in the early centuries.”⁹⁶² The Nigerian courts have continually applied the English common law in matters that have not been legislated into federal or state laws in “so far... as the limits of local circumstances shall permit”.⁹⁶³ The common law will, therefore, apply in matters that have not been covered by legislation.⁹⁶⁴

The law of torts does not recognise an invasion of privacy as a form of tortious liability. There has been a growing recognition of the invasion of privacy as a tort in England in the last decade. Under the English law, plaintiffs whose privacy have been infringed could make use of other torts such as trespass, nuisance, libel and malicious falsehood.⁹⁶⁵ These other torts, however, provide abysmally insufficient relief and are

⁹⁵⁹ Chapter 5, sec. 5.2.

⁹⁶⁰ Abdulrauf and Daibu “New Technologies and the Right to Privacy in Nigeria: Evaluating the Tension between Traditional and Modern Conceptions”, 2016 7 *Nnamdi Azikiwe University Journal International Law and Jurisprudence* 125, 126; Tobi *Sources of Nigerian Law (1996)* 17-58; Obilade *The Nigerian Legal System (1979)* 69-82; Olong *The Nigerian Legal System 2ed (2007)* 11-20; Mwalimu *The Nigerian Legal System (2009)* 27-29; Taiwo and Akintola, *Introduction to Equity & Trusts in Nigeria (2016)* 30.

⁹⁶¹ Nwauche, 2007 1 *CALS Review of Nigerian Law and Practice* 67.

⁹⁶² Abdulrauf and Daibu 2016 7 *NAUJILJ* 121.

⁹⁶³ S.32(1) of the Interpretation Act Cap 123, Laws of Federation of Nigeria (LFN) (2004).

⁹⁶⁴ Adigun, “Enforcing ECOWAS Judgments in Nigeria through the Common Law Rule on the Enforcement of Foreign Judgments” 2019 15 *Journal of Private and International Law*” 137.

⁹⁶⁵ *Wright v Home Office* [2003] United Kingdom House of Lords 53, 16 October 2003.

inadequate to protect all aspects of privacy.⁹⁶⁶ For example, invasion of privacy caused by intrusion, such as communications surveillance, does not usually fit into the category of any of these torts.⁹⁶⁷ Another example is the use of breach of confidence to claim damages for invasion of privacy.⁹⁶⁸ A successful claim through the breach of confidence involves evidence of a confidential relationship between the parties. The breach of confidence is, therefore, inadequate to cover all aspects of invasion of privacy, particularly in respect of intrusions on privacy such as communications surveillance.⁹⁶⁹

Nigerian jurisprudence has yet to recognise a tort of invasion of privacy. This may be because the 1999 Nigerian Constitution recognises a right to privacy and provides monetary compensation as a constitutional relief for an infringement of a fundamental right but only as a punitive measure.⁹⁷⁰ This is unlike the jurisprudence in South Africa where monetary compensation for an infringement of the right to privacy can be claimed under the law of delict as discussed in chapter three. Scholars, including Laosebikan and Nwauche, have advocated for the development of a tort of privacy by the courts by emulating the developing English jurisprudence.⁹⁷¹

⁹⁶⁶ McGonagle "A Tort of Privacy: The Privacy Bill" 2006 *Quarterly Review of Tort Law* 2.

⁹⁶⁷ Markesinis *et al* 2004 *AJCL* 142; Singh and Strachan "Privacy Postponed" *European Human Rights Law Review Special Edition: Privacy* 25. In *Kaye v Robertson and Sport Newspapers Ltd* [1991] FSR 62 (U.K), the pictures of the plaintiff, a well-known actor, were taken from the hospital where he was recovering from a car accident by a tabloid journalist who pretended to be someone else. The plaintiff instituted several torts unsuccessfully to restrain the photographs from being published and to claim damages. The plaintiff only succeeded on the claim of malicious falsehood at the Court of Appeal with a grossly inadequate relief that exempted the publication from stating that the pictures were taken with the plaintiff's consent; in *Bernstein of Leigh v Skyviews and General Ltd*, [1978] QB 479, the plaintiff unsuccessfully claimed damages for trespass for a "clear case of snooping and unacceptable aerial surveillance". In some cases, the Court, for example in *Khorasandjian v Bush* [1993] QB 479, was open to stretching the law of tort to cover invasion of privacy but it majorly depends on the willingness of the judge; *Tolley v Fry* [1931] AC 333; *Re X* [1984] 1 WLR 1422; *Imerman v Tchenguiz* (2011) Fam 116 par [65]; *Campbell v MGN* (2004) UKHL 22.

⁹⁶⁸ Solove "'I've got nothing to hide' and other misunderstandings of privacy" 2007 44 *San Diego Law Review* 770; Abdulrauf *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* (doctoral thesis, University of Pretoria) 2015 127.

⁹⁶⁹ Nwauche, 2007 1 *CALS Review of Nigerian Law and Practice* 77.

⁹⁷⁰ *Emerging Markets Telecommunications Services Limited v Eneye* (2018) LPELR-46193 (CA) 29; *Ibironke v MTN Nigeria Communications Ltd* (2019) LPELR-47483 (CA) 35.

⁹⁷¹ *WB v H Bauer Publishing Ltd* (2002) Entertainment and Media Law Reports 145; Nwauche, Lindsay and Ricketson "Copyright, Privacy and Digital Rights Management" in AT Kenyon & M Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 121; Laosebikan *Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in Internet Cafes and Suggestions for Appropriate Legislation in Nigeria* (doctoral thesis, Howard College School of Law, University of Kwazulu-Natal, Durban) 2007, 333-334; Abdulrauf and Daibu 2016 7 *NAUJILJ* 126; *Coco v AN Clark (Engineers) Ltd*

Nwauche states that claims for compensation for the infringement of the right to privacy against non-State actors are difficult.⁹⁷² This opinion may be because of the confusing jurisprudence on the horizontality of the Bill of Rights at the time. There have been some clarifications in this regard in recent times. The Court of Appeal in *Emerging Markets Telecommunications Services Limited v Eneye*⁹⁷³ held a non-state actor liable for invasion of privacy. The court declared that the continuous sending of unsolicited messages constitutes an infringement of privacy and awarded monetary compensation. Hence, non-State actors can be held liable for an infringement of the right to privacy and pay compensation to victims if the court orders constitutional damages.⁹⁷⁴

Notwithstanding this commendable decision of the court providing clarity on the horizontality of the Bill of Rights, there is still a need for the development of the tort of privacy. The global evolution of new means to invade privacy through intrusive collation of data and/or disclosure of information by new technologies contributes to the urgency of a need for a tort of privacy by the court. It is more likely for the courts to catch up with the rapidly evolving innovations in ICT than it is for the legislature to enact laws.⁹⁷⁵ There is still no statute on the protection of data privacy, there is however a recent regulation providing protection to data privacy, that is the NDPR. This is however subordinate legislation and moreover fragmented provisions in various statutes on the protection of data privacy. These fragmented provisions are industry-

(1969) Report of Patent Cases 41, 47; Solove DJ “‘I’ve Got Nothing to Hide’ and other Misunderstandings of Privacy” 2007 44 *San Diego Law Review* 770; Philipson “Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act” 66 2003 *Modern Law Review* 726.

⁹⁷² Nwauche *et al* “Copyright, Privacy and Digital Rights Management” (2006) 125; Laosebikan *Privacy and Technology Development* (2007) 333.

⁹⁷³ *Emerging Markets Telecommunications Services Limited v Eneye* (2018) LPELR-46193 (CA) 29; *Ibironke v MTN Nigeria Communications Ltd* (2019) LPELR-47483 (CA) 35.

⁹⁷⁴ Constitutional damages are awarded for an infringement of human right and usually punitive. Tortious damages are compensation to person who suffers damage as a result of a tortious act with the aim of restoring the injured person to the position they were before the damage. *Emerging Markets Telecommunications Services Limited v Eneye* (2018) LPELR-46193 (CA) 34; Delia-Mihaela “Aspects regarding Tortious Civil Liability for the Deeds of Minors” 2021 *Proceedings of the International Conference of Law, European Studies an International Relations* Section C 364.

⁹⁷⁵ It is acknowledged that there are consequences of courts developing the law and not merely interpreting it. Where courts develop the law it may lead to legal uncertainty and blurring the barriers between the judiciary and legislature (impacting on the separation of powers rule). Nevertheless, the judiciary can be a bridge between the people and the legislature in fields where there is no legislation. Dafel *The Constitutional Rebuilding of the South African Private Law: A Choice between Judicial and Legislative Law-Making* (doctoral thesis, University of Cambridge) 2018) 8-10.

specific; they do not reflect current global trends in data privacy protection and will supersede where there is a conflict with the NDPR.

Additionally, constitutional damages cannot adequately provide compensation for all cases of invasion of privacy. While the court may declare that there is an infringement of the right to privacy, the plaintiff may fail to convince the court to award constitutional damages.⁹⁷⁶ One of the grounds for the granting of constitutional damages and which is most likely to apply horizontally is a situation where the defendant makes a calculated effort to make profit that exceeds the compensation payable to the plaintiffs and this may be difficult to prove.⁹⁷⁷ Whereas if invasion of privacy becomes a tortious liability, the plaintiff who has suffered damage must be compensated by the defendant in a claim for unliquidated damages.⁹⁷⁸ The burden of proof on the plaintiff requires evidence that damage has occurred that must be compensated.

The South African approach is different from Nigeria's common law. Instead of a different tort, each with their own requirements as seen in Nigeria, the South African jurisprudence utilises general principles of delict to determine delictual liability.⁹⁷⁹ Nevertheless, South African law recognises liability for invasion of privacy under the common law. The South African jurisprudence has also been able to unify both the constitutional and common law concepts of privacy to provide a suitable redress for invasion of privacy.⁹⁸⁰ Nigeria should similarly expand its jurisprudence on privacy and not limit its jurisprudence to public remedies alone. This can be possible by the development of a tort of privacy that will provide private law remedies. The public law

⁹⁷⁶ *Enanuga v Sampson* (2012) LPELR-8487 (CA) 20.

⁹⁷⁷ *Ibid.*

⁹⁷⁸ Gligorijevic "A Common Law Tort of Interference with Privacy for Australia Reaffirming ABC v Lenah Game Meats" 2021 44 *University of New South Wales Law Journal* 693; Giliker "A Common Law Tort of Privacy? – The Challenges of Developing Human Rights Tort" 2015 27 *Singapore Academy of Law Journal* 764-766; Richards "The Limits of Tort Privacy" 2011 9 *Journal on Telecommunications & High Technology Law* 358.

⁹⁷⁹ *S v A* 1971 (2) SA 293 (T) 298; *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 463; *Sage Holdings Ltd v Financial Mail (Pty) Ltd* 1991 (2) SA 117 (W) 129, 130; *Motor Industry Fund Administrators (Pty) Ltd v Jamit* 1994 (3) SA 56 (W) 61; Neethling *et al Personality Rights* 314; Neethling and Potgieter *Law of Delict* 425.

⁹⁸⁰ Chapter 3, sec.3.7.3; S.39(2) of the Constitution; *NM v Smith* 2007 (5) SA 250 (CC) par [31]; South African Law Commission "Discussion Paper 109, Project 124 on Privacy and Data Protection" (October 2005) <https://www.justice.gov.za/salrc/dpapers/dp109.pdf> 5 (Chapter 2) (accessed on 2020-2-11); Currie and De Waal *The Bill of Rights Handbook* 31, 41- 42; Dafel *The Constitutional Rebuilding of the South African Private Law: A Choice Between Judicial and Legislative Law-Making* (2018) 63.

remedies can then be applied when the State infringes on the right to privacy unlawfully and without excluding private law remedies if necessary.

The global evolution of new means to invade privacy through intrusive collation of data and/or disclosure of information by new technologies that may not have been defined under the constitutional right to privacy contributes to the need for a tort of privacy by the court. However, the Court of Appeal in *Emerging Markets Telecommunications Services Limited v Eneye* has recently held a non-state actor liable for infringement of the right to privacy based on the continuous sending of unsolicited messages and also awarded monetary compensation.⁹⁸¹ The court awarded damages to the respondent for an infringement of his fundamental rights.⁹⁸²

This indicates that, rather than developing a tort of privacy, the court will award constitutional damages. The court has through this suit shown that the Bill of Rights applies horizontally. It can only be hoped that the Supreme Court will decide on matters challenging non-state parties to infringement of rights in order to resolve the confusing decisions on horizontality of the Bill of Rights.

4.8 Laws regulating communications surveillance in Nigeria

There are two models of legal framework employed for the regulation of communication surveillance in Nigeria. These are statutes and subsidiary legislation in the form of institutional regulatory guidelines.⁹⁸³ The statutes regulating interception of communications are the Nigerian Communications Act, 2003, the Cybercrimes (Prohibition and Prevention) Act, 2015 (CPPA) and the Terrorism (Prevention and Prohibition) Act, 2022 (TPPA). The Nigerian Communications Commission (NCC) was established by the Nigerian Communications Act, 2003 (NCA), which also empowers it to make regulations relating to electronic communications in Nigeria. The NCC, in line with provisions of the NCA that empowers it to make subsidiary legislation, passed the Lawful Interception of Communications Regulation, 2019.

⁹⁸¹ *Emerging Markets Telecommunications Services Limited v Eneye* 34.

⁹⁸² *Ibid.*

⁹⁸³ There are different provisions impacting on the right to privacy in some Nigerian statutes. These provisions protect the right to privacy as it correlates with the objects of the statute or the industry that the statute regulates. They also do not have provisions on communications surveillance and not relevant to this thesis. They are therefore not addressed. These statutes are the Freedom of Information Act, 2011, the Child's Right Act, 2003, the National Identity Management Commission Act, 2007, National Health Act, 2014, the Federal Competition and Consumer Protection Act, 2019 and the Credit Reporting Act, 2017.

The National Information Technology Development Commission through its empowering statute, the National Information Technology Development Act, 2007 (NITDA), developed the Nigerian Data Protection Regulation (NDPR), 2019 that regulates the protection of personal data in Nigeria. The NDPR does not provide for communications surveillance, but it provides for the protection of personal data and the processing of personal data as part of the communication surveillance process. The NDPR, through its provisions for the protection of personal data, therefore, indirectly regulates the post-surveillance aspect of communications surveillance that deals with processing of data.

The CPPA, TPPA and the LICR refer to interference relating to the content of communication and/or its metadata as interception of communication. This is unlike the South African legislation, RICA, which defines interception of communication as any interference with the content of communication.⁹⁸⁴ Interference with metadata is referred to in the RICA as real time and/or archived communication-related information.⁹⁸⁵ The CPPA, TPPA and the LICR provide for targeted communications surveillance and so does the RICA, even though different terminologies are used.⁹⁸⁶

There is very little evidence on whether bulk surveillance is utilised in Nigeria.⁹⁸⁷ The possibility of bulk surveillance is only inferred with reference to sophisticated surveillance equipment recorded in Nigeria's national budget.⁹⁸⁸ None of the statutes or regulations provide for bulk surveillance. The execution of bulk surveillance is, therefore, unlawful and contravenes section 45(1) of the 1999 Nigerian Constitution. The relevant laws for the regulation of communication surveillance in Nigeria will now be considered.

⁹⁸⁴ S.1 of 70 of 2002.

⁹⁸⁵ S.1 of 70 of 2002.

⁹⁸⁶ S.58 of 19 of 2020; Regulation 23 of the Lawful Interception of Communications Regulation.

⁹⁸⁷ Deeks "An international legal framework for surveillance" 2015 55 *Virginia Journal of International Law* 292; Milanovic "Human rights treaties and foreign surveillance: Privacy in the digital age" 2015 56 *Harvard International Law Journal* 81; Abdulrauf "The Challenges for the Rule of Law Posed by the Increasing Use of Electronic Surveillance in Sub-Saharan Africa" 2018 18 *African Human Rights Law Journal* 369.

⁹⁸⁸ Abdulrauf 2018 18 *AHRLJ* 370; Emmanuel "Exclusive: Jonathan awards \$40 million contract to Israeli company to monitor computer, internet communication by Nigerians" *Premium Times* (25 April 2013) <https://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-to-israeli-company-to-monitor-computer-internet-communication-by-nigerians.html> (accessed 2017-06-10).

4.8.1 Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015

The Cybercrimes (Prohibition, Prevention, Etc.) Act (CPPA) provides for the “protection of critical national information infrastructure...computer systems and networks, electronic communications data and computer programs, intellectual property and privacy rights”.⁹⁸⁹ It also seeks to promote cybersecurity and provide a legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution, investigation and punishment of cybercrimes in Nigeria.⁹⁹⁰ The CPPA is a comprehensive law for matters relating to the prohibition, prevention and prosecuting of cybercrimes in Nigeria.⁹⁹¹ The CPPA also classifies any crime that relates to electronic communication and computer networks, amongst others, as a cybercrime and this includes the unlawful interception of communications.⁹⁹² The CPPA provides that the offence of unlawful interception of communication is committed by:

“[a]ny person, who intentionally and without authorization, intercepts by technical means, non-public transmissions of computer data, content, or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network.”⁹⁹³

The offence of interception of communication, for example in South Africa, generally relates to interception over an electronic communications network. In the CPPA, the offence of unlawful interception of communications includes the interception of credit or debit card details.⁹⁹⁴ Unlawful interception of communications also involves the interference with a computer system that is not connected to any electronic network. Section 9 of the CPPA provides for the offences of intercepting of electronic messages, emails and electronic money transfers. The offence of unlawful interception of communication in the CPPA is, therefore, broader than the interference of communications over an electronic communications network.

Section 38 of the CPPA provides that a CSP shall retain the metadata and subscriber information for a period of two years.⁹⁹⁵ This information forms part of the personal information of subscribers for a period of two years. The CSP is obligated to intercept

⁹⁸⁹ S.1(b) and (c) of the CPPA.

⁹⁹⁰ S.1(a) of the CPPA.

⁹⁹¹ S.1(a) of the CPPA.

⁹⁹² Ss.6-16 of the CPPA.

⁹⁹³ S.12(1) of the CPPA.

⁹⁹⁴ S.12(2) of the CPPA.

⁹⁹⁵ S.38(1) CPPA.

and/or provide subscribers information, content and metadata of communications at the request of authorised law enforcement officers and the NCC.⁹⁹⁶ The content of electronic communications can be intercepted only with the authorisation of an interception order by the Federal High Court.⁹⁹⁷ However, acquisition of metadata does not require judicial authorisation and is, therefore, less protected than the content of communications.⁹⁹⁸ This is similar to the current position in South African law.⁹⁹⁹ Many European countries also provide less protection for metadata. However, the current global position is that metadata is as intrusive as content of electronic communications and should be protected equally.¹⁰⁰⁰

The CPPA provides for the utilisation of interception of the content of communications for all crimes even though its purpose relates to cybercrimes only.¹⁰⁰¹ The CPPA provides that the utilisation of interception of the content of communications can only be used for the “purposes of criminal investigation and proceedings”.¹⁰⁰² It also states that acquisition of metadata must be for legitimate purposes under the CPPA, any other statutes or regulation.¹⁰⁰³ It does not provide for specific purposes for the use of metadata acquisition. The CPPA, by being specific about what constitutes legitimate purposes for interception of content of communication and not metadata, provides a better safeguard for the former.

⁹⁹⁶ Ss.38, 39 and 50 of the CPPA.

⁹⁹⁷ S.39 of the CPPA.

⁹⁹⁸ S.38 of the CPPA.

⁹⁹⁹ Ss.9, 15 and 19 of 70 of 2002.

¹⁰⁰⁰ An analysis of metadata can reveal information that includes a person’s movements at any given time, both virtual and physical contacts, time of contact, social circles, intimate relationships, routines, religious beliefs and interactions with protected sources or confidential clients. Report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014; Report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014; Court of Justice of the European Union, Judgment in joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger* Judgment of 8 April 2014; *AmaBhungane v Minister of Justice* par [28], the High Court stated that RICA was enacted based on “what was understood to be the character of the telecommunications environment of that time”; Right to Know and Privacy International “The Right to Privacy in South Africa: Stakeholder Report Universal Periodic Review, 27th Session, South Africa” (October 2016) 5; Crockford “Graphs by MIT Students Show the Enormously Intrusive Nature of Metadata” (7 January 2014) www.aclu.org/blog/national-security/secretcy/graphs-mit-students-show-enormously-intrusive-nature-metadata (accessed on 2020-01-30); Privacy International <https://privacyinternational.org/education/data-and-surveillance> (accessed on 2020-01-30).

¹⁰⁰¹ S.39(1) of the CPPA.

¹⁰⁰² *Ibid*; S.39(1) of the CPPA.

¹⁰⁰³ Ss.38(4) and (5) of the CPPA.

The utilisation of interception of communications may be justified under section 45(1) of the 1999 Nigerian Constitution either as a means of maintaining public order or preserving the rights and freedom of persons through crime prevention. The international law position is that it is unreasonable to intercept communications in order to investigate non-serious crimes.¹⁰⁰⁴ The aim of the utilisation of communications surveillance is therefore legitimate only if applied to serious crimes.¹⁰⁰⁵ Otherwise, it is not reasonably justifiable.

Section 45(1) of the CPPA provides that a judge shall grant a warrant for the purpose of obtaining electronic evidence for any criminal investigation in relation to the Act. The judge must be convinced that there are reasonable grounds to believe that an offence under the CPPA has been or is about to be committed.¹⁰⁰⁶ Even though the CPPA provides that interception of communication can be executed for all crimes, procedural guidelines are provided to the judge in respect of cybercrimes.¹⁰⁰⁷

The application for a warrant to intercept or obtain content and/or metadata of an electronic communication is made *ex parte*.¹⁰⁰⁸ The CPPA, however, does not provide for the information that the application must contain and whether the judge is empowered to request additional information. Hence, the CPPA does not specifically empower the judge to full access of all information pertaining to the application for an intercept warrant.

The CPPA does not also specifically prevent the judge from requesting further information on the application. The applicant for an intercept warrant has a duty to convince the judge to grant the warrant thus indicating that the application for a warrant can be refused where the judge is not satisfied with the evidence supporting the

¹⁰⁰⁴ Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 39th session, agenda items 2 and 3, A/HRC/39/27, 3 August 2018 par [38].

¹⁰⁰⁵ These crimes are considered serious crimes as provided in the Schedule to the RICA and recommended for Nigeria as crimes that can prompt surveillance in chapters five and six. They include high treason, any offence relating to terrorism, any offence involving sabotage, sedition, any offence that could result in the loss of a person's life or serious risk of loss of life, racketeering, criminal gang activities, dealing in drugs, dealing in or smuggling of ammunition, firearms, explosives or armament, any offence the punishment whereof may be imprisonment for life or a period of imprisonment exceeding five years without an option of fine. Also, the offences referred to in articles 6, 7 and 8 of Rome Statute of the International Criminal Court.

¹⁰⁰⁶ S.45(2) of the CPPA.

¹⁰⁰⁷ *Ibid.*

¹⁰⁰⁸ S.45(1) of the CPPA.

application.¹⁰⁰⁹ This may be a safeguard against preventing law enforcement officers from applying for warrants without cause. Since information supporting an *ex parte* application is required to be provided under oath, the applicant may be deterred from fabricating evidence as he/she will be liable for perjury.¹⁰¹⁰

Because the application for an interception warrant is made *ex parte*, the accused persons are unable to defend themselves.¹⁰¹¹ Since it is not clear from the provisions of the CPPA whether judges are empowered to demand access to all information concerning the application, they are not in the best position to protect the right to privacy of the surveillance subject. The CPPA empowers judges to act as adjudicator over surveillance matter, hence the surveillance subjects are unable to defend themselves. The right to a fair hearing of the surveillance subject is therefore unjustifiably infringed.¹⁰¹²

It would have been better if the CPPA had empowered judges to act in an inquisitorial capacity, which would give them access to all information concerning the application. This will enable judges to conduct a proportionality test considering all the information before them and arrive at a well-reasoned decision wherein the protection of surveillance subject's human rights in the most effective manner is paramount.

The CPPA does not provide for post-surveillance notification, thus, the subjects of surveillance are not in a position to challenge the infringement of their rights. The judge in an application for an intercept warrant is, therefore, the guardian of the fundamental rights of the subject of surveillance. The judge is responsible to ensure that the decision is not prejudicial to any party in the suit.¹⁰¹³ The court as the guardian of constitutional rights requests full access to information where necessary when considering the *ex parte* application for an intercept warrant.

The CPPA, being a statute that focuses on criminal procedure relating to cybercrimes, is not a regulatory law for communications surveillance in Nigeria. Its provisions only relate to the criminal justice procedure relating to cybercrimes. It therefore does not

¹⁰⁰⁹ S.45(3) of the CPPA.

¹⁰¹⁰ *Kotoye v Central Bank of Nigeria* (1989) LPELR-1707 (SC) 84.

¹⁰¹¹ S.45(1) of the CPPA.

¹⁰¹² Chapter 4, sec.4.8.4.3.8. It is acknowledged that the justification for an *ex parte* application is also subject to various safeguards that ensures that the subject of surveillance has a fair hearing. In the absence of these safeguards the right to fair hearing will be unjustifiably infringed.

¹⁰¹³ *Sheldon v Broomfield* (1964) 2 Q.B. 578; *Kotoye v Central Bank of Nigeria* 32; *Adigun v AG, Oyo State* 678; *Deduwa v Okorodudu* (1974) 1 All NLR (Pt.1) 272 (SC).

adequately protect fundamental rights or provide procedural guidance on the execution of communications surveillance in Nigeria.

4.8.2 Terrorism (Prevention and Prohibition) Act, 2022

The Terrorism (Prevention and Prohibition) Act, 2022 (TPPA) repeals the Terrorism (Prevention) Act, 2011 and the Terrorism (Prevention)(Amendment) Act, 2013. The TPPA aims to provide a unified legal, regulatory and institutional framework for the

“detection, prevention, prohibition, prosecution and punishments of acts of terrorism, terrorism financing, proliferation and financing the proliferation of weapons of mass destruction in Nigeria.”

The TPPA defines an act of terrorism as any wilfully performed act that intends to further an ideology and that may cause serious harm to and intimidate people of a country. It also includes any act that unduly compels or coerces the government to perform an act or refrain from performing the act and seriously destroys or destabilises the government.¹⁰¹⁴

Section 68(1) of the TPPA provides as follows in respect of interception of communications:

“Without prejudice to any other law, a relevant agency may, with the approval of National Security Adviser for the purpose of the –

- (a) prevention of acts of terrorism or the commission of any other offence under this Act,
- (b) enhancement of the detection of offences related to the preparation of an act of terrorism, or
- (c) the prosecution of offenders under this Act,

apply *ex-parte* to the Court for an “interception of communication order.”

The provision of section 68 of the TPPA, unlike the CPPA, has an internal administrative mechanism that ensures that application for an interception order is made with the approval of the national security office. The application for an interception of communication order under the TPPA has more procedural guidelines than the CPPA.

The TPPA empowers the Court, which is a Federal High Court judge, to make a decision about the duration of validity of the interception warrant.¹⁰¹⁵ If the Court is not aware of the global standards on surveillance warrants, he/she is likely to be convinced

¹⁰¹⁴ S.2(3) of the TPPA.

¹⁰¹⁵ Ss. 29(3) and 99 of the TPPA.

to issue a warrant for a longer duration than necessary. International and foreign law, for example RICA, on the matter of the duration of surveillance provides for three months, which is renewable.¹⁰¹⁶ The TPPA provision gives unlimited discretion to the Court and the absence of a provision for renewal leaves the execution of the surveillance order unsupervised. This encourages abuse by LEAs.

In comparison, in the RICA, the application for a renewal enables the judges to review the execution of the prior order.¹⁰¹⁷ The absence of this procedure in the TPPA indicates that there is no safeguard against abuse of the communications surveillance order once it is authorised. The LICR is more current on the global requirements in this regard and it provides for the duration of an intercept warrant as three months, renewable for another three months.¹⁰¹⁸

Section 68(4) of the TPPA provides that intercepted information shall be admissible in proceedings relating to the offences under the TPPA “as evidence of the truth of its content”. The section contains an irrebuttable presumption that intercepted communications correspond with the actual message sent by the originator. Section 3 of the Evidence Act, 2011 provides that “[n]othing in this Act shall prejudice the admissibility of any evidence that is made admissible by any other legislation validly in force in Nigeria.”¹⁰¹⁹ However, section 153(2) of the Evidence Act states that an intercepted communication is rebuttable evidence of the actual content of the message. Section 153(2) of the Evidence Act and section 68(4) of the TPPA are therefore conflicting provisions. It is submitted that the Evidence Act should supersede the TPPA in this case, as the purpose of the Evidence Act is to prescribe admissibility of evidence in all judicial proceedings in Nigeria.

It is noted that the rule of interpretation of statute is that where there is a conflict between two pieces of legislation one of which is specific on a subject and the other

¹⁰¹⁶ *Huvig v France*, App. No. 11105/84 (1990) par [34]; *Amann v Switzerland*, App. No. 27798/95, (2000) par [76]; *Bugallo v Spain*, App. No. 58496/00, (2003) par [30]; S.16(6)(d) of 70 of 2002.

¹⁰¹⁷ S.16(6)(d) of 70 of 2002.

¹⁰¹⁸ Regulation 14(1)-(5) of the LICR.

¹⁰¹⁹ S.153(2) of the Evidence Act of Nigeria, 2011 provides that “[t]he court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the court shall not make any presumption as to the person to whom such message was sent”.

which is general in nature, the specific legislation shall supersede.¹⁰²⁰ Nonetheless, section 68(4) of the TPPA cannot be considered as a special provision because it does not possess any distinguishing factor from the CPPA and the LICR, both of which regulate communications surveillance and do not have a similar provision. The LICR, being the only law dedicated primarily to interception of communication in Nigeria, provides that interception information can only be admissible in evidence subject to the consent of the Presiding Judge on the matter.¹⁰²¹

Additionally, the aim of the TPPA is the criminal justice procedure relating to terrorism-related offences, thus communications surveillance is only consequential to the aim of the Act. Furthermore, the TPPA does not provide any reasons for communications surveillance utilised for terrorism-related investigation to be an exception to the general rule in section 29(4) of the Evidence Act. It is submitted that in the absence of any special circumstance that separates the evidence obtained from communications surveillance in terrorism-related investigations from other very serious crimes, the provisions of the Evidence Act supersede that of the TPPA.

Intercepted information, whether obtained lawfully or unlawfully, is admissible in evidence at the discretion of the court.¹⁰²² Section 68(4) of the TPPA does not make the information obtained lawful, it only provides for weight to be placed on the content of the intercepted communication in evidence. The lawfulness of the intercepted communication can, therefore, still be challenged and the court has the discretion to admit or reject the evidence.

The TPPA, like the CPPA, does not provide a detailed procedural guideline or regulation on all execution of communications surveillance. The TPPA only focuses on ensuring that there is no interference with law enforcement officers in the exercise of their duties regarding terrorism related matters. It is, therefore, not a law that can regulate the execution of all forms of communications surveillance in Nigeria.

¹⁰²⁰ *Madume v Okwara* (2013) LPELR 20752 (SC) 15-17; *Attorney General of Ogun State v Attorney General of the Federation* (2003) FWLR (Pt.143) 206; *Edet Akpan v The State* (1986) 3 NWLR (Pt.27) 25; *Aqua Ltd v Ondo State Sports Council* (1988) 4 NWLR (Pt.9) 622.

¹⁰²¹ Regulation 17 of the LICR.

¹⁰²² S.14 of the Evidence Act provides that “evidence obtained improperly or in contravention of a law... shall be admissible unless the court is of the opinion that the desirability of admitting the evidence is outweighed by the undesirability of admitting evidence that has been obtained in the manner in which the evidence is obtained”.

4.8.3 Nigerian Communications Act, 2003

The main objective of the Nigerian Communications Act (NCA) is to regulate all matters related to the Nigerian communications industry and establish the Nigerian Communications Commission.¹⁰²³ The NCA also has a mandate to protect the rights and interests of CSPs and their consumers.¹⁰²⁴ The NCA empowers the NCC to make regulations and guidelines on matters listed in section 70(1)(a)-(g).¹⁰²⁵ These matters include licensing for CSPs, issues relating to communications and related offences and penalties and “such other matters as are necessary for giving full effect to the provisions of this Act and for their due administration”.¹⁰²⁶

Section 70(g) of the NCA provides that the NCC can make regulations on “such other matters as are necessary for giving full effect to the provisions of this Act and for their due administration”. This means that the matters on which the NCC can make laws are not limited to those in section 70(a)-(e). The term “such other” also implies that the items listed in section 70(a)-(e) are matters that are necessary to give full effect to the NCA and its administration. Matters that are not provided for in the NCA are not within the regulatory ambit of the NCC.

As a result of its powers to make subsidiary legislation, the NCC formulated the LICR. The NCC is an executive branch of the government that is answerable to the Minister of Communications, and ultimately, to the President. Regulation by the NCC on matters like the interception of communications, that regulates the powers of the executive, should not be formulated by the executive as it defeats the purpose of separation of powers. It is tantamount to the executive regulating itself and may allocate unfettered powers to the President and his cabinet. Also, section 1 of the NCA specifies the aim of the statute as providing a regulatory framework for the Nigerian communications industry and all matters related to it. This indicates that the aim of the NCA is to provide a regulatory mechanism and in line with that, the NCC was established as the regulatory body. The provisions of the NCA focus on the manner in which the NCC can facilitate the relationship between the State, CSPs and their customers. It is not within the ambit of the NCA to provide a legal framework for law

¹⁰²³ S.1 of the Nigerian Communications Act.

¹⁰²⁴ S.1(g) of the Nigerian Communications Act.

¹⁰²⁵ S.1(b) of the Nigerian Communications Act.

¹⁰²⁶ S.70 (a)-(g) of the Nigerian Communications Act.

enforcement matters.¹⁰²⁷ The NCC, therefore, cannot allocate powers that the NCA does not itself appropriate as it did with the LICR, which is discussed in the next subsection.

The NCC states that its powers to formulate the LICR stem from sections 146 and 147 of the NCA. Section 146 and 147 empower the NCC to determine when and how a CSP can activate the technical capacity to intercept communications. Section 146 (1) and (2) of the NCA provide that:

“(1) A licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content application service that he provides from being used in, or in relation to, the commission of any offence under any law in operation in Nigeria.
(2) A licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as 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.”

The NCA provides for the obligation of CSPs to intercept communications as required by the statute. It states the two circumstances in which a CSP, through the provisions of the NCA, can permit interception of communications on its network. The first circumstance is where interception of communications is executed by the CSPs as a way to prevent their network facilities from being utilised to commit an offence under any law in Nigeria.¹⁰²⁸ Secondly, the CSP may assist the NCC or other authority upon a written request to intercept communication for the purpose of preventing an offence or enforcing the laws in Nigeria.¹⁰²⁹ Section 146(3) of the NCA exempts the CSP from any criminal liability of any nature for any act or omission “done in good faith” while utilising their network to prevent crimes. Unlike the LICR, it does not, however, exempt them from civil liability.¹⁰³⁰

The provision of section 146 is problematic for the following reasons: firstly, empowering the CSP and the NCC in preventing the utilisation of the network to prevent the commission of offences amounts to encroaching on the duty of law

¹⁰²⁷ A legal framework on communications surveillance must be “established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive”. Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 27th session, agenda items 2 and 3, A/HRC/27/37, 30 June 2014, par [29].

¹⁰²⁸ S.146(1) of the NCA.

¹⁰²⁹ S.146(2) of the NCA.

¹⁰³⁰ Regulation 4 of the LICR.

enforcement agencies.¹⁰³¹ It would be preferable that they report such incidents, rather than prevent the occurrence themselves. Neither CSPs nor NCC are trained to carry out law enforcement duties, hence their involvement in law enforcement matters for the purpose of crime prevention is an overreach of their ambit.¹⁰³²

Secondly, section 146(2) of the NCA does not specify the exact authority that can intercept communications. This signifies that any organ of the State, for example, broadcasting authorities like the Nigerian Television Authority, can intercept communications insofar as the purpose is to prevent a crime. The provision of section 146(2) of the NCA is too broad, and susceptible to abuse. Thirdly, the power to intercept communications is not subject to any independent oversight mechanism.

Lastly, the legitimate aim for interception of communications provided for in section 146(2) of NCA is broader than the limitation provided for in section 45(1)(a) and (b) of the 1999 Nigerian Constitution. The protection of public revenue is not a legitimate aim to limit the fundamental rights in section 45(1)(a) and (b) of the 1999 Nigerian Constitution.

In the same vein, Section 147 of the NCA provides that:

“The Commission may determine that a licensee or class of licensee shall implement the capability to allow authorised interception of communications and such determination may specify the technical requirements for authorised interception capability.”

The powers conferred on the NCC in section 147 relates to the implementation of the technical capacities that enable interception of communications on the network of CSPs. Section 147 cannot be the basis for which the NCC derives the power to provide a legal framework for interception of communications under the LICR. The NCC is authorised by section 147 to specify the technical requirements, not provide the legal framework, for interception of communication.¹⁰³³ In light of the above problems, section 146 and 147 of the NCA are too broad. It is not reasonably justifiable in a

¹⁰³¹ Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 27th session, agenda items 2 and 3, A/HRC/27/37, 30 June 2014, par [3]. International law’s requirement regarding communications surveillance highlighted in the 2014 report of the OHCHR indicates that governments habitually threaten to deny CSPs of the renewal of their licenses if they do not follow their instructions which are usually unlawful; In spite of this, the NCA has specifically empowered CSPs to undertake law enforcement duties.

¹⁰³² S.4 of the Nigerian Police (Establishment) Act, 2020.

¹⁰³³ Regulation 2 of the Lawful Interception of Communications Regulation.

democratic society to limit fundamental rights in the course of intercepting communications.

In light of the powers conferred on the NCC to make subsidiary legislation, other regulations, aside from the LICR, relating to processing of personal information of customers of CSP were formulated. The NCC formulated the Consumer Code of Practice Regulation, 2007 (CCPR) and the Registration of Telephone Subscriber Regulation, 2011 (RTSR).¹⁰³⁴ The CCPR regulates the procedures for the preparing of consumer codes by CSPs.¹⁰³⁵ Regulation 35 of the CCPR also provides for the protection of personal information of consumers by the CSPs. The CCPR also provides for the general principles of processing of personal information.¹⁰³⁶ These include fair and lawful collection, prohibition of excessive collection, accurate and up to date information, and information not being kept longer than necessary.¹⁰³⁷ The CCPR regulates only CSPs and does not apply to other persons, such as the State processing personal information.¹⁰³⁸

The RTSR regulates persons who subscribe to a mobile telephone service in Nigeria to ensure their registration and proper management of the database.¹⁰³⁹ Subscriber information collected by the CSPs has to be transferred to a central database managed by the State.¹⁰⁴⁰ The information can be accessed by security agencies only after a written request has been made to the NCC.¹⁰⁴¹ Regulation 9 of the RTSR provides that in line with section 37 of the 1999 Nigerian Constitution that protects the right to privacy, subscribers be permitted to assess their information on the central database and update and/or amend it.¹⁰⁴² The information in the central database will not be released to a CSP, security agent or the subscriber if the request breaches any provision of the 1999 Nigerian Constitution or any Act of the National Assembly and/or a threat to national security.¹⁰⁴³

¹⁰³⁴ Consumer Code of Practice Regulation 2007, GN 56 in GG 87, Vol.94 of 2007-07-10; Nigerian Communications Commission (Registration of Telephone Subscriber Regulation) 2011, GN101 in GG 229, Vol. 98 of 2011-11-07.

¹⁰³⁵ Regulation 2 of the CCPR.

¹⁰³⁶ Regulation 35 of the CCPR.

¹⁰³⁷ *Ibid.*

¹⁰³⁸ Regulation 1 of the Schedule to the CCPR (General Consumer Code of Practice).

¹⁰³⁹ Regulation 2 and 3 of the RTSR.

¹⁰⁴⁰ Regulation 6 of the RTSR.

¹⁰⁴¹ Regulation 8 of the RTSR.

¹⁰⁴² Regulation 9(1) of the RTSR.

¹⁰⁴³ Regulation 10(2) of the RTSR.

Neither the CCPR nor the RTSR make provision for the protection of personal information provided to law enforcement agencies in the course of communications surveillance. This is because their focus is on the regulation of the use of electronic communications among CSPs. The LICR, discussed in the next subsection, is the only law that focuses on regulating the interception of communication in Nigeria.¹⁰⁴⁴

4.8.4 Lawful Interception of Communications Regulation, 2019

The Lawful Interception of Communications Regulation (LICR), 2019 is subsidiary legislation promulgated by the NCC by virtue of section 70 of the NCA, that provides that the NCC “may make and publish regulations for” the matters specified in section 70(1)(a) -(g).¹⁰⁴⁵ The LICR, unlike the CCPR, does not state the specific matters in section 70 of the NCA that empowers them to regulate interception of communications. The NCC clearly states in the CCPR that their powers to make the regulation are derived from section 4(1)(b) and (p) of the NCA.¹⁰⁴⁶ Stating the specific provision of the enabling statute on which a subsidiary legislation is based, aids the persons making the law to keep within the scope of the delegated powers. As discussed below, the LICR exceeds its ambit; nevertheless, the court is mandated to take judicial notice of subsidiary legislation that is available in a matter before it.¹⁰⁴⁷ Courts will, therefore,

¹⁰⁴⁴ Regulation 1 of the LICR.

¹⁰⁴⁵ Regulation 1(a)-(g) of the Lawful Interception of Communications Regulation provides as follows: “[t]he Commission may make and publish regulations for all or any of the following issues:

- (a) Written authorisations, permits, assignments and licences granted or issued under this 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 this 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.

¹⁰⁴⁶ Regulation 1(2) and 2 of the CCPR provides as follows:

“1(2) Specifically these Regulations are made pursuant to section 106 of the Act and the functions of the Commission identified in Sections 4 (1) (b) and 4 (1) (p) of the Act.

2 The specific objectives of these Regulations are to:

- confirm and clarify the procedures to be followed by Licensees in preparing approved consumer codes of practice in accordance with section 106 of the Act; and to determine and describe the required contents and features of any consumer code prepared by, or otherwise applicable to, Licensees.”

¹⁰⁴⁷ S.122(1) and (2) of the Evidence Act provides that:

“1 No fact of which the court shall take judicial notice under this section needs to be proved.

2 The court shall take judicial notice of – (a) all laws and any subsidiary legislation made under them having the force of law now or previously in force in any part of Nigeria;”.

consider the LICR as one of the laws regulating interception of communications in Nigeria.¹⁰⁴⁸

4.8.4.1 Structure of the Lawful Interception of Communications Regulation

The LICR provides that the interception of communication is lawful when it is executed by authorised agencies listed under Regulation 23.¹⁰⁴⁹ It also provides that interception of communication is lawful where a party to the communications consents to the interception.¹⁰⁵⁰ Interception of communications is also lawful when executed with an interception warrant. Interception of communication is further lawful when it is executed by a party to the communication on the belief that “there is a threat to human life and safety”.¹⁰⁵¹ In addition, interception of communication that occurs in the ordinary course of business that requires monitoring or record of such communication is lawful.¹⁰⁵² Authorised agencies also have the power to request for the keys or code of an encrypted message and CSPs must provide it on request.¹⁰⁵³ CSPs must also comply with section 147 of the NCA and ensure that they install interception capabilities on their networks as directed by the NCC.¹⁰⁵⁴

The LICR provides for targeted interception of communication only, as signified by the definition of interception in Regulation 23 of the LICR. LICR does not provide for bulk (untargeted) interference and neither does any law in Nigeria. The utilisation of bulk interference in Nigeria is, therefore, an infringement of the right to privacy as it is not supported by law in line with section 45(1) of the 1999 Nigerian Constitution.

The next subsection discusses the qualities of the LICR and analyses whether it adequately protects the right to privacy and other rights involved in communications surveillance. The second subsection discusses the problems with the LICR.

4.8.4.2 Potentially sound provisions in the LICR

Regulation 7(2) and (3) of the LICR provide guidelines for judges on information to consider before the application for a warrant is approved. These guidelines are absent in the CPPA and the TPPA. These provisions guide the court on grounds to consider

¹⁰⁴⁸ *Ibid.*

¹⁰⁴⁹ Regulation 4 of the LICR.

¹⁰⁵⁰ Regulation 8(a) of the LICR.

¹⁰⁵¹ Regulation 8(b) of the LICR.

¹⁰⁵² Regulation 8(c) of the LICR.

¹⁰⁵³ Regulation 9 of the LICR.

¹⁰⁵⁴ Regulation 10 and 11 of the LICR.

when evaluating an application for an interception warrant. It also states the legitimate purposes that may require an interception warrant. Although some of the legitimate purposes, as discussed in the next subsection, do not align with section 45(1) of the 1999 Nigerian Constitution, there was still an effort by the framers of the LICR to restrict the utilisation of interception of communication for specified purposes.

Regulation 12 of the LICR, like section 1 of the RICA, provides for the designation of persons qualified to apply for an interception warrant.¹⁰⁵⁵ Only the National Security adviser or his assignee and the Director of the State Security Service or his assignee may apply for an interception warrant.¹⁰⁵⁶ In addition, only the designated persons within the authorised agencies may have access to intercepted communications.¹⁰⁵⁷ The LICR also provides that an interception warrant will only be issued where interception of communication is the only means of obtaining the required information.¹⁰⁵⁸ These provisions reduce unnecessary applications for an interception warrant and thereby reduce the workload on the judges. Nevertheless, as discussed in the next subsection, the application for a warrant is only optional and has little impact on the adequate safeguard of fundamental rights.

The Federal High Court has jurisdiction over surveillance applications. The Federal High Court judges, like other judges, are appointed by the National Judicial Council and are independent of the executive.¹⁰⁵⁹ The judiciary possesses the requisite independence required for surveillance matters. The discussion in chapter two indicates that the judiciary may be the most desirable option for an independent oversight mechanism.¹⁰⁶⁰ However, they may be ineffective to safeguard fundamental

¹⁰⁵⁵ Regulation 12(1) of the LICR provides that “[p]ursuant to the provisions of section 148 (1) (c) of the Act, an application for a warrant under these Regulations shall be made to the Judge by any of the following Agencies—

(a) the Office of the National Security Adviser represented by the National Security Adviser or his designee, who shall not be below the equivalent of an Assistant Commissioner of Police; and

(b) the State Security Services represented by the Director or his designee, who shall not be below the equivalent of an Assistant Commissioner of Police.”

¹⁰⁵⁶ *Ibid.*

¹⁰⁵⁷ Regulation 18(3) of the LICR.

¹⁰⁵⁸ Regulation 12(3)(e) of the LICR.

¹⁰⁵⁹ S.7(2) of the LICR.

¹⁰⁶⁰ *Dumitru Popescu v. Romania (no. 2)*, App. No. 71525/01, (2007) par [71]; *Zahkarov v Russia* pars [233, 258].

rights if they are not properly trained on the special nature of surveillance matters and they do not possess full access to information.¹⁰⁶¹

Regulation 13(2) provides that an interception warrant is directed to an authorised agency and only authorised persons within the agency are permitted to execute interception or handle intercepted information. Regulation 14(1) of the LICR provides that a warrant shall be valid for three months and it is renewable for another three months upon an application for such renewal. Regulation 14(1) provides safeguards that ensure that the interception of communication does not continue indefinitely and the court can monitor the process by ensuring that it does not continue indefinitely.

4.8.4.3 Problems with the LICR

Section 2(e) of the LICR provides that one of the objectives of the LICR is to “ensure that the privacy of subscribers’ communication as provided for in the Constitution of the Federal Republic of Nigeria is preserved”. The LICR as analysed in this section is very problematic and Regulation 2(e) indicates that there is no recognition that the right to privacy is not the only right infringed in the process of interception of communication.

4.8.4.3.1 Overreach into the exclusive legislative list

Regulation 4 of the LICR provides that “[i]t shall be lawful for any Authorised Agency listed in Regulation 12(1) of these Regulations to intercept any Communication or pursuant to any legislation in force”. Authorised agencies listed in Regulation 12(1) of the LICR are the Nigeria Police Force, the National Intelligence Agency, the State Security Services, the Economic and Financial Crimes Commission and the National Drug Law Enforcement Agency. In addition, the NCC can add other agencies to the list of authorised persons as it deems fit.

The regulation of interception of communications by its very nature includes regulating law enforcement agencies’ utilisation of electronic communications in criminal procedure and intelligence matters. These are sensitive matters that are designated for the Exclusive Legislative List. The power to make laws regarding wireless communications, police, defence, military and external matters is in the Exclusive

¹⁰⁶¹ *Zakharov v Russia* par [260]; *Association for European Integration and Human Rights and Ekimdzhiev* pars [79-80].

Legislative List of the National Assembly and cannot be delegated.¹⁰⁶² The LICR, therefore, overreached its ambit by regulating the manner in which law enforcement agencies conduct their duties.

The licensee, in addition to permitting interception of communications and/or disclosure of the intercepted communication, is also required to comply with any international mutual assistance agreement and this usually includes interception of communication by foreign agencies. Regulation 7(1)(c) makes provision that relates to external affairs and which is also in the Exclusive Legislative List of the National Assembly and beyond the purview of a subsidiary legislation.

4.8.4.3.2 Broad powers of law enforcement agents

Regulation 4 of the LICR defines lawful interception of communication as one:

- “(i) that is conducted by an authorised agency;
- (ii) that in relation to other legislation, relates to interception of a communication service provided by a licensee to a person in Nigeria or outside Nigeria”

The parameters for lawful interception in terms of the above description are related to whoever conducts the interception and whether the service provider is licensed in Nigeria. Interception of communications is lawful simply because it is conducted by an authorised agency or provided for in a statute in Nigeria. The ECtHR has stated that one of the purposes of ensuring quality laws for communications surveillance is to curb the actions of overzealous law enforcement officers.¹⁰⁶³ Regulation 4 of the LICR has widely exposed the fundamental rights of persons to the arbitrariness of law enforcement officers. As discussed later on,¹⁰⁶⁴ the LICR provides for a judicial oversight mechanism. Regulation 4 creates the impression that the judicial oversight mechanism is optional. It would have been better to define lawful interception as being executed by a warrant before the matter of authorised persons to apply for a warrant is addressed.

Regulation 4 of the LICR also exempts CSPs from any civil or criminal liability that may be incurred as a result of permitting persons authorised by law to conduct communications surveillance. The NCA only exempts CSPs from criminal liability and, therefore, the LICR exceeded its power by including exclusion from civil liability.¹⁰⁶⁵

¹⁰⁶² Schedule 1, Exclusive Legislative List 1999 Nigerian Constitution.

¹⁰⁶³ *Zakharov v Russia* par [270].

¹⁰⁶⁴ Chapter 4, sec. 4.8.4.3 (v).

¹⁰⁶⁵ S.146(3) of the NCA.

Regulation 5 classifies any interception of communication conducted outside of the provisions of the LICR or any legislation in Nigeria as an offence. The punishment of the offence, however, is not specified in the LICR.

4.8.4.3.3 Inadequate protection of personal information

Regulation 6 provides for storage of intercepted communication. Authorised agencies are required to store intercepted communications.¹⁰⁶⁶ The LICR does not state where, how and for how long the information obtained through interception of communication has to be kept. The authorised agencies in possession of the intercepted communication have to destroy all intercepted communication that is not admitted into evidence. The LICR does not specify how the intercepted information admitted in evidence is to be processed or how it should be treated after the conclusion of the trial.¹⁰⁶⁷

Regulation 6(3) provides that intercepted communication is to be kept confidential, however, the procedure that ensures confidentiality is not specified. Section 6(3) also provides that only the content of communication may be shared and for the purpose of criminal investigation only or it must be archived for three years and then destroyed. The use of “or” means that it is stored for the purpose of the criminal investigation and then archived for three years and destroyed thereafter. The provision, therefore, omits the duration for which information shared for criminal investigation must be kept before it is destroyed.

In addition, it does not explain the purpose for archiving intercepted information that is not utilised for criminal investigation and thereby breaches the NDPR.¹⁰⁶⁸ Since the purpose of acquiring intercepted information is for criminal investigation, any other purpose constitutes unlawful processing of personal information and an unjustifiable infringement on the right to privacy. Regulation 6(4) of the LICR provides that information that is not relevant shall be extracted and the non-relevant part removed. There is no time limit regarding when the relevant part must be removed or when the non-relevant part is to be destroyed. The processing of intercepted information is unlawful to the extent that the LICR does not provide for procedures that ensure protection of personal data. One of the requirements of a law, according to global

¹⁰⁶⁶ Regulation 6(1) of the LICR.

¹⁰⁶⁷ Regulation 6(1) of the LICR.

¹⁰⁶⁸ Regulation 3.1 of the NDPR.

standard, that adequately protects fundamental rights is that it minimises the risk of abuse at every stage.¹⁰⁶⁹ The LICR does not reflect this requirement.

Regulation 16 of the LICR prohibits disclosure of information obtained from the interception of communication to unauthorised persons. Regulation 19 also provides that logged information on interception shall only be disclosed if there is a court order for its disclosure. There is, however, no offence created or any penalty for unauthorised disclosure of information obtained from the interception. Therefore, while the CSPs have specific fines for refusal to cooperate with authorised persons for communications surveillance, authorised persons incur no liability for disclosure of information. This also indicates that the LICR is more interested in enabling communications surveillance than protecting the fundamental rights affected.

Regulation 19 of the LICR provides that law enforcement agencies are to submit monthly reports to the NCC and quarterly reports to the Attorney General of the Federation on interceptions executed.¹⁰⁷⁰ While this may seem commendable in theory, it does not practically alleviate the many risks of abuse in the LICR. This is because there is no provision detailing the NCC or AGF's response to this report, hence it is not known whether the reports are for accountability purposes or for record keeping.

4.8.4.3.4 Optional warrant for interception of communication

Regulation 7 of the LICR provides for the duty of the licensee to comply with the order in an interception warrant.¹⁰⁷¹ This provision does not state whether an authorised agent may only intercept with a warrant. It only provides that CSPs must comply with the order of a warrant. Regulation 7 suggests that where the CSP is not opposed to the interception of its network without a warrant then it is not necessary to intercept communication. Regulation 7 further buttresses the argument in section 8.4.3(b) above, that the lawfulness of interception of communication is dependent on whether it is executed by an authorised agency. The LICR again has shown that its priority is

¹⁰⁶⁹ *Zakharov v Russia* par [233]; *Bigbrother Watch v UK* par [309].

¹⁰⁷⁰ Regulation 19 of the LICR.

¹⁰⁷¹ Regulation 7(1) of the LICR provides as follows:

“(1) Subject to these Regulations, a Licensee shall act upon a warrant issued by a Judge authorising or requiring the Licensee to whom it is addressed to comply with the provisions of the warrant, to secure any one or more of the following”.

to enable the interception of communications rather than the protection of fundamental rights.

In addition, CSPs have no reason to oppose the interception of communications as they are exempted from any liability that may arise. A CSP who opposes the provisions of the Regulation is liable to a fine of N5, 000, 000 or the revocation of their license. The CSPs are more likely to suffer grievous loss for obstructing the interception of their network when it is without a warrant.¹⁰⁷² The LICR again exceeded its ambit as the penalty of the sum of N5, 000, 000 exceeds the penalty limit of six months imprisonment and/or N100 prescribed as maximum penalty limit for subsidiary legislation in the Interpretation Act.¹⁰⁷³

Regulation 7 of the LICR further provides that a warrant shall only be granted “provided that there is no other lawful means of investigating the matter for which the warrant is required”. Regulation 7 would have been a safeguard for fundamental rights as it provides for interception of communication as a last resort. However, with a warrant being an optional exercise, it cannot practically provide the intended safeguard.

4.8.4.3.5 Lack of clarity on the definition of unlawful interception of communication

Regulation 7(2) provides that a judge can only issue a warrant where it is necessary for the purposes stated in Regulation 7(3). Regulation 4 of the LICR provides that interception of communication is lawful when executed by an authorised agency. On the other hand, Regulation 7 provides that a warrant can be granted when information required may only be obtained through lawful interception. If the interception of communications is lawful because it is executed by an authorised agency, why then would an authorised agency need a warrant to obtain information that is already lawful, by virtue of their position as an authorised person? It seems that the NCC wants to include a supervisory body but at the same time does not want law enforcement agencies to be subject to supervision. Otherwise, a lawful interception should have first been defined as one that is executed with a warrant. The LICR, therefore, lacks clarity on the definition of unlawful interception of communication.

¹⁰⁷² Regulation 16 of the Lawful Interception of Communications Regulation.

¹⁰⁷³ S.12(1)(c)(ii) of the Interpretation Act, Cap 123, Laws of Federation of Nigeria (LFN) (2004).

The discussion in chapter three indicates that the RICA, even though enacted as far back as 2002 and while imperfect, provides clearly that interception of communication can only take place with a warrant issued by specified courts.¹⁰⁷⁴ The RICA also indicates clearly and in detailed specification, the persons (not agencies), authorised to intercept communications and the type of information that such persons are empowered to intercept.¹⁰⁷⁵ The provisions of the RICA, in this regard, are appropriate for Nigeria to emulate.

4.8.4.3.6 Purposes for interception of communications infringe on the 1999 Nigerian Constitution

Regulation 7(3) also provides for activities that a warrant is required for and they are:

- “(a) it is in the interest of the national security as may be directed by the persons listed in regulation 12(1) (a) or (b) of these Regulations;
- (b) for the purpose of preventing or investigating a crime;
- (c) for the purpose of protecting and safeguarding the economic well-being of Nigerians;
- (d) in the interest of public emergency or safety; or
- (e) giving effect to any international mutual assistance agreements, to which Nigeria is a party.”

Regulation 7(3)(c) and (e) of the LICR does not align with the legitimate purposes for the limitation of the rights in section 45(1) of the 1999 Nigerian Constitution. An interception of communications based on section 7(3)(c) and (e) of the LICR is, therefore, an infringement of fundamental rights in section 45(1) of the 1999 Nigerian Constitution. Regulation 7(3)(b) also provides that communications surveillance can be executed for “a crime”, hence indicating that any kind of crime whether serious or not can require an interception warrant. This is a very broad aim for the utilisation of communication surveillance and makes room for arbitrariness.

The discussion in chapter two signifies that the intrusive nature of communications surveillance is such that its execution must be utilised for serious crimes only. UN General Comments and the ECtHR have stated that any utilisation of communications surveillance short of serious crimes is an inappropriate utilisation of communications

¹⁰⁷⁴ Ss.16(1), 17(1) and 19(1) of 70 of 2002.

¹⁰⁷⁵ S.1 of 70 of 2002.

surveillance and arbitrary.¹⁰⁷⁶ The RICA and the G 10 Act are examples of statutes that align with the international law and the ECtHR in this regard.¹⁰⁷⁷

4.8.4.3.7 Inadequate experience of Judges on the special nature of intercept warrants

Regulation 13(3) of the LICR provides that a Judge of the Federal High Court is the specified judicial official to grant an intercept warrant. It does not indicate any specialised training on interception matters like the designated judges in the RICA. The Judges of the Federal High Court and those of the State High Court have concurrent jurisdiction and are on the same hierarchical level in the judicial structure. There is, therefore, no reason why judges of the State High Court cannot also sit on surveillance matters. The important issue, as specified by the ECtHR, is not the cadre of the judges but their specialised training and expertise on surveillance matters.¹⁰⁷⁸

It is crucial that judges presiding over surveillance matters understand that an interception warrant is not like other warrants. The defendants in other types of warrants such as search warrants are able to challenge the warrants because they eventually become aware when the warrants are executed against them. Subjects of surveillance, on the other hand, may never be aware of the surveillance without a post-surveillance notification and their right to a fair hearing is denied. Hence, judges presiding on surveillance matters cannot be adjudicators. The duty of judges in this respect, as discussed in chapters two and three of this thesis, is inquisitorial as they act as the guardian of the people's fundamental rights.¹⁰⁷⁹ Their duty in surveillance matters is, therefore, to determine the best way to safeguard the fundamental rights of the subject under surveillance.

Furthermore, the information in support of the application is not preserved under oath and as such the applicant is not criminally liable should the information provided be false.¹⁰⁸⁰ The applicant is given the discretion to decide what information to reveal or

¹⁰⁷⁶ Annual Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, 39th session, Agenda items 2 and 3, A/HRC/39/27, 3 August 2018 par [38]; *Kopp v Switzerland* par [64]; *Valenzuela Contreras v Spain*, App. No. 58/1997/842/1048 (1998), par [46]; *Malone* par [67]; *Huvig v France* par [29]; *Weber and Saravia* pars [103-106]; *Bigbrother Watch* par [308].

¹⁰⁷⁷ S.16(5) of 70 of 2002.

¹⁰⁷⁸ *Zahkarov v Russia* par [250]; *Kennedy v United Kingdom*, No. 26839/05 par [161]; *Klass v Germany* par [52]; *Weber and Saravia v Germany* par [98].

¹⁰⁷⁹ S.16(7)(b) of 70 of 2002.

¹⁰⁸⁰ Regulation 3(a)-(d) of the LICR.

withhold. This does not provide an avenue for an overzealous officer to be held criminally responsible as incorrect information provided under oath may lead to a charge of perjury. The only information required to be under oath is a statement that interception of communication is the only means of obtaining the required information.¹⁰⁸¹

Regulation 13(a) of the LICR provides that a judge may only issue an interception warrant where the facts alleged are reasonable and persuasive enough. This indicates that an overzealous applicant who requires a successful warrant can provide false information since this is all alleged and it is not under oath. Law enforcement agents in Nigeria have been widely criticised for their abuse of powers. As there is no mechanism to verify the information provided, it is unlikely that law enforcement officers will provide information that may result in an unsuccessful outcome for their application.

The discussion in chapter three of this thesis is useful to provide guidance to Nigeria in this regard. Section 16 of the RICA provides a detailed guidance to judicial officers on information that is required to safeguard the rights of the defendant adequately. Section 16 (7)(b) of the RICA also provides specifically that judicial officers can request additional information where the information provided by the applicant of an interception direction is inadequate. The RICA ensures that the judicial officers are granted full access to information in order to determine the level of infringement on the subject of surveillance that is reasonable and justifiable in the circumstance. This is instructive for Nigeria in ensuring that judges understand that in a surveillance matter they are empowered to request full access to information.

The RICA's appointment of designated judges by cabinet members was criticised in chapter three as not providing the adequate independence oversight mechanism required for surveillance matters. However, the designated judges are experienced jurists who are retired and they have the time to concentrate only on surveillance matters, unlike regular judges.

¹⁰⁸¹ Regulation 3(e) of the LICR.

4.8.4.3.8 Application for warrant infringes unjustifiably on the right to fair hearing

The application for an interception warrant is made *ex parte* and the defendant do not have an opportunity to defend themselves.¹⁰⁸² The *ex parte* nature of the application may be justifiable before and during the interception of communications because of the secrecy required for the process to be effective.¹⁰⁸³ The justification for the *ex parte* is also subject to various safeguards that ensures that the subject of surveillance has a fair hearing.

The Court of Appeal in *Akuma Industries v Ayman Enterprises Ltd* declared on the nature of an *ex parte* application as follows:

“Common sense and decency and the concept of civilised behaviour dictate that before the majesty of the court parties must be at per at the hearing of a case. Indeed, *Anton Pillar* although seemingly appearing as a monstrosity has become accepted within the vortex or [*sic*] our legal doctrine...the order made should not be so overwhelming as to exhaust the case and render the later argument on the case a waste of time.”¹⁰⁸⁴

This signifies that *ex parte* orders, such as Anton Piller orders, should only be granted in extreme circumstances and with caution as the order is granted based on the applicant’s statement only. Communications surveillance orders may be justifiable in this regard, if precautions are taken and safeguards are provided for human rights.

The South African Constitutional Court declared in *Amabhungane* that the notification of the surveillance subject after the surveillance is one of the safeguards that must be provided to ensure fair hearing.¹⁰⁸⁵ The LICR does not provide for post-surveillance notification even though the application is *ex parte*. The LICR also does not provide any avenue to ensure a fair hearing of the surveillance application. Consequently, the procedure for authorisation of a communications surveillance order which is through *ex parte* application is an unjustifiable limitation on the right to a fair hearing of the surveillance subject.

¹⁰⁸² Regulation 13(4) of the LICR.

¹⁰⁸³ *Independent Newspaper (Pty) Ltd v Minister for Intelligence Services: In Re Masetlha v President of the Republic of South Africa* 2008 (5) SA 31 (CC) par [45].

¹⁰⁸⁴ (1999) LPELR-13412 (CA) 34.

¹⁰⁸⁵ *AmaBhungane v Minister of Justice* (CC) par [44-47]; *AmaBhungane v Minister of Justice* par (GP) [74] “the condition upon which the secret spying process can be justified, ie fundamental values are reluctantly trampled on, with as light a tread as possible”.

A post-surveillance notification as discussed in chapters two and three of this thesis avails the subject of surveillance of the opportunity to seek redress where there is an unjustifiable infringement on his fundamental rights. It also enables the subject of surveillance to challenge the inadequacy of surveillance laws while seeking redress. Section 46(1) of the 1999 Nigerian Constitution also provides for the right to seek redress where there is an infringement of fundamental rights. The absence of post-surveillance notification to subjects of surveillance in the LICR is, therefore, an unjustifiable infringement on the right to seek redress and in conflict with the 1999 Nigerian Constitution.

4.8.4.3.9 Unjustifiable infringement on the right of access to court

Regulation 20(1) of the LICR provides that anyone or any CSP who is aggrieved with an interception activity “shall” notify the NCC and “may” apply for judicial review. The words utilised signifies that it is compulsory to notify the NCC. The LICR does not state how the NCC is required to handle the complaints. It also does not empower the NCC to act as an administrative review for the interception activity. The judicial review to the court is an additional appendage to the complaint made to the NCC.¹⁰⁸⁶

A person who applies for judicial review may do so through the fundamental rights enforcement procedure discussed in section 4b above. This will ensure an expedited review of such interception. However, the clandestine nature of surveillance makes it almost impossible for subjects of surveillance to be aware of interception activities. It is, therefore, unlikely that subjects of surveillance will apply to court for judicial review. The provision for judicial review is, therefore, ineffective to guarantee right of access to court for redress in the absence of a post-surveillance notification.

The ECtHR included a requirement that consideration of surveillance must be on a case-by-case basis.¹⁰⁸⁷ This allows the judge to determine whether post-surveillance notification is suitable in the circumstance or the duration of its delay. The importance of an experienced and specialised independent oversight mechanism is crucial on this matter. A judge who is experienced in handling surveillance matters will be in a better position to evaluate when denying access to court for the subject of surveillance is justifiable and when it is not. The NCC is not in a position to provide adequate redress

¹⁰⁸⁶ Regulation 20(1) of the LICR.

¹⁰⁸⁷ *Weber and Saravia v Germany* pars [51,133-135]; *Klass v Germany* par [19]; *Zakharov v Russia* par [289].

since it is neither independent nor experienced in judicial matters. The NCC is, therefore, not a competent authority with the jurisdiction for fundamental rights enforcement.

In light of the above, the LICR as a law regulating the interception of communication in Nigeria does not provide adequate safeguards for fundamental rights. It is more of an enabling law for the execution of interception of communications than a law that protects fundamental rights. The structure of oversight mechanism, even though independent, is insufficient to act as a guardian of fundamental rights. Personal information is also minimally protected and there is little provision that indicates justifiable processing of information in all aspects of the surveillance process. The LICR also exceeded its ambit as provided in the NCA and went overboard into the Exclusive Legislative List of the National Assembly.

The LICR further exceeded the legitimate aims for limitation of rights as provided in section 45(1) of the 1999 Nigerian Constitution. The LICR also conflicts with other statutes and has unclear provisions regarding what constitutes unlawful interception. The LICR lacks clarity, provides very broad powers to law enforcement agencies, and provides inadequate safeguards for fundamental rights. It therefore does not provide safeguard against arbitrariness.

4.8.5 Nigerian Data Protection Regulation, 2019

The Nigerian Data Protection Regulation (NDPR), 2019 was formulated by the National Information Technology Development Agency (NITDA), which was created by the National Information Development Agency Act (NITDA Act). The function of the NITDA among others is to regulate all matters relating to information technology. It is also responsible for developing guidelines for electronic governance and monitoring electronic data.

The scope of the NITDA in relation to data protection is limited to electronic data only. Regardless of this limited scope, the NITDA formulated the NDPR as the law regulating data protection in Nigeria. The NDPR defines personal data (personal information) as any information relating to an identified or identifiable natural

person.¹⁰⁸⁸ The personal data that the NDPR protects relates to both electronic and non-electronic data. One of the objectives of the NDPR is to:

“ensure that Nigerian businesses remain competitive in international trade; through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which regulatory framework is in tune with global best practices.”¹⁰⁸⁹

The NDPR provides the legal regulatory framework on data protection in Nigeria even though the NITDA is empowered to regulate matters relating to information communication and by extension electronic data only. The NITDA, therefore, exceeded the power conferred on it by the NITDA Act by regulating non-electronic data. Nevertheless, the NDPR is currently the comprehensive law that protects personal data in Nigeria.¹⁰⁹⁰

The NDPR provides that processing of personal data for public interest or “in exercise of official public mandate” is lawful.¹⁰⁹¹ The activities of the State regarding interception of communication constitutes lawful processing as it is utilised for criminal law activities in law enforcement. The processing of information obtained during interception of communications is lawful. However, the processing of personal data of the subjects of surveillance is not. This is because the information is not processed in line with governing principles of lawful processing provided in the NDPR.¹⁰⁹²

Unlike the POPIA that exempts certain activities of State from its scope, the NDPR does not exempt the State from any of its provisions. It provides that anyone who is in possession of personal data of a data subject must be accountable for any acts or omissions while processing data in line with the NDPR.¹⁰⁹³ In addition, all public and private organisations that are in control of personal data of natural persons are subject to the regulation of the NDPR.¹⁰⁹⁴ They must also provide a data protection policy to the public. Ultimately, the State is to comply with principles of data processing in the NDPR in order to ensure the protection of personal data.

¹⁰⁸⁸ Regulation 1.3(q) of the NDPR.
¹⁰⁸⁹ Regulation 1.0 (d) of the NDPR.
¹⁰⁹⁰ Regulation 1.0 (a) of the NDPR.
¹⁰⁹¹ Regulation 2.2 (e) of the NDPR.
¹⁰⁹² Regulation 2 of the NDPR.
¹⁰⁹³ Regulation 2.1(3) of the NDPR.
¹⁰⁹⁴ Regulation 3.1 of the NDPR.

The NCC in formulating the NDPR did not consider the peculiar situation of the State with regard to the clandestine nature of surveillance wherein consent of the data subject will defeat the purpose. In addition, both the NDPR and the LICR are subordinate legislation and cannot nullify actions that are permitted in a statute. Where a statute permits processing of personal data that is against the processing principles in the NDPR, the provisions of the statute will prevail over the NDPR. The CPPA and the TPPA does not provide for processing of personal data in the execution of interception of communication. Law enforcement officers are, therefore, subject to the NDPR in processing the personal information of subjects of surveillance.

4.9 Conclusion

The legal framework of communications surveillance in Nigeria, like South Africa, has its root in the 1999 Nigerian Constitution. Section 37 provides for a right to privacy, albeit for Nigerian citizens only. It therefore discriminates against non-Nigerians. This notwithstanding, it provides for the protection of the right to privacy in very broad terms, and which enables courts to provide an interpretation of the right to privacy that accommodates global changes and technological advancements. New challenges to privacy such as data privacy and communications surveillance are adequately protected under the umbrella of the right to privacy when interpreted broadly and flexibly.

While the 1999 Nigerian Constitution adequately protects the right to privacy, its limitation clause hampers the practical protection of the right. Several difficulties arise from the current interpretation of section 45(1) of the 1999 Nigerian Constitution. One of the problems is the restrictive phrases used in the contextual formulation of the limitation clause. Phrases like “[n]othing in section... shall”, “any law” and “reasonably justifiable”, that do not have interpretive guidance in the 1999 Nigerian Constitution impede its flexible interpretation. Many judicial decisions err precariously on the side of restricting the fundamental rights, rather than advancing them.

At the same time the various laws limiting the right to privacy as well as empowering communications surveillance are vague and overreach. The result is that they empower the State to limit rights unreasonably. Very few decisions have attempted to apply section 45(1) of the 1999 Nigerian Constitution in a manner that adequately limits the scope of such laws to advance the protection of fundamental rights and

curtail State powers. Part of the problem is that section 45(1) lacks a uniform guideline of interpretation that permits objectivity while balancing the right to privacy as well as the other rights mentioned in section 45(1) against State powers.

This state of affairs has enabled the State, through subsidiary legislation, to promulgate laws that unjustifiably limit rights. These laws, like the LICR and the NDPR that affect the right to privacy and surveillance, do not only minimally protect the right, but they also overreach their ambit into the exclusive domain of the National Assembly. For example, the NCC erroneously empowers itself to formulate a legislative framework on communications surveillance, that is the LICR.

As shown in chapters two and three, communications surveillance is a tool utilised in law enforcement duties. Regulating communications surveillance is tantamount to regulating law enforcement duties, yet the NCC as an organ of the State, has sought to regulate State power by disregarding the purpose of separation of powers. As expected, the LICR has garnered vast power in favour of the State in order to permit communications surveillance with minimal independent supervision.

The State is also not held responsible for arbitrary infractions on fundamental rights. This creates a very low threshold for the protection of fundamental rights in the execution of communications of surveillance. The NCC, through the LICR, has also made itself the main oversight mechanism for the regulation of the communications surveillance in Nigeria. The LICR provides in unclear and uncertain terms that the court also serves as an oversight mechanism. However, a holistic analysis of the LICR signifies that invocation of the jurisdiction of the court over surveillance matters is optional for law enforcement officers.

Furthermore, the LICR overextends its ambit by providing a vast number of purposes for which communications surveillance may be executed. These are far more than those constitutionally permitted by section 45(1)(a) and (b) of the 1999 Nigerian Constitution. For example, the LICR includes purposes, such as economic wellbeing and enabling international mutual assistance, neither of which are legitimate aims for limiting fundamental rights provided for in the 1999 Nigerian Constitution, and which can be broadly interpreted. The LICR is, therefore, inconsistent with the 1999 Nigerian Constitution, to the extent that it includes of the illegitimate aims for communications surveillance. In addition, the LICR does not provide for the protection of personal

information during the surveillance process. Ultimately, the LICR as the main legal framework on communications surveillance in Nigeria is inadequate to safeguard fundamental rights and minimise arbitrariness.

The CPPA and the TPPA are statutes that provide for communications surveillance in addition to their focus, namely the prevention, detection and prosecution of cybercrimes and terrorism respectively. These statutes neither protect the right to privacy, nor provide procedural guidelines for the execution of communications surveillance. Neither the CPPA nor the TPPA are adequate as the primary statutes on communications surveillance in Nigeria.

Linked to the four thematic areas identified throughout the thesis, it is clear that the LICR, CPPA and TPPA as a Nigerian legal framework for communications surveillance does not adequately safeguard human rights. First, a comprehensive statute regulating communications surveillance is of utmost importance for the protection of human rights and for alignment with the 1999 Nigerian Constitution. The statute like the RICA should focus on protecting fundamental rights in the course of executing communications surveillance. This is needed to ensure a primary statute for communications surveillance, with clearly defined terms and provisions, to create legal certainty.

Secondly, a statute similar to the South African RICA is needed to ensure clear links between the protection of fundamental rights during the execution of communications surveillance. A comprehensive statute must also provide for safeguards for the protection of the right to privacy at every stage of surveillance. Currently, the Nigerian laws are unclear regarding the appropriate procedure for an application for a surveillance warrant as each of the laws have conflicting provisions. There is no provision in any of the laws in respect of the procedures for the execution of a surveillance warrant. The result is that LEAs have unlimited access to the communications of subscribers to a communications network.

Thirdly, none of the laws provide for post-surveillance notification and a surveillance subject therefore has no recourse in court, because he or she is usually unaware of the surveillance. It is thus very important that proper procedural structures are put in place for the implementation of communications surveillance in Nigeria.

Finally, the communications surveillance regime in Nigeria also lacks experienced oversight mechanisms. Even though judges are experienced in the interpretation of law, they are not best suited as oversight bodies for surveillance process without further training on the peculiarities of surveillance. This is evidenced by the grant of surveillance warrants on an *ex parte* basis, without an accompanying date for post-surveillance notification to enable the surveillance subject to challenge the process. Specialised oversight bodies, are therefore, required to ensure that there are adequate safeguards at all stages of the surveillance process. Furthermore, none of the laws provide an avenue for redress for the surveillance subject hence infringing on the right to access to court of the surveillance subjects. Reform is clearly needed.

In the next chapter, the analysis of the problems with the Nigerian laws on communications surveillance is undertaken and is linked to the five main issues already identified, namely: the interpretation of section 45(1) of the 1999 Nigerian Constitution; a comprehensive statute for communications surveillance; effective procedural guidelines at all stages of the surveillance process; efficient and effective oversight bodies; and an avenue for redress. The chapter uses relevant international and regional law and the South African law, as set out in chapters two and three respectively, to guide the recommendations for reform of the Nigerian legal framework on communications surveillance.

CHAPTER FIVE

RECOMMENDATION FOR A HUMAN RIGHTS BASED LEGAL FRAMEWORK ON COMMUNICATIONS SURVEILLANCE FOR NIGERIA

5.1 Introduction

The previous three chapters discussed the state of communications surveillance regulation in international law, selected regional law, South Africa and Nigeria. It was established that the right to privacy is the primary right that is infringed during communications surveillance, because such surveillance is only possible by infringing communications privacy. This means that it is critical to examine how the limitation of the right to privacy through communications surveillance can be justified.

Chapter four confirmed that section 37 of the 1999 Nigerian Constitution provides for a right to privacy and, specifically, communications privacy. The precise provision in the Constitution on the protection of communications privacy needs no special interpretation by the court, as it is clearly stated. The court also interprets section 37 in a manner that extends to data privacy.¹⁰⁹⁵ This is commendable, because communications surveillance limits both communications and data privacy.

The right to privacy is not absolute and is limited by section 45 of the Constitution. However, unlike section 37, section 45 does not provide clarity on how to balance the right with its limitation. The result, as discussed in chapter four, is that in most cases Nigerian courts do not conduct a proportionality evaluation to determine whether a law limiting section 45 rights is reasonably justifiable. Government interests often supersede the protection of these rights.¹⁰⁹⁶ This ultimately implicates the legitimacy of the communications surveillance regime in Nigeria.

The existing position, as discussed in chapter four, is that the only criterion that is considered by Nigerian courts during a section 45 adjudication is that a legitimate aim is met. This approach imperils human rights as it neglects the balancing exercise that ought to be conducted in determining whether the laws limiting rights are reasonably justifiable. It is a clear that in order to make full recommendations for the reform of the

¹⁰⁹⁵ *Nwali v Ebonyi State Independent Electoral Commission* (2014) LPELR-23682 (CA) 60.

¹⁰⁹⁶ Chapter 4, section 6.

Nigerian law on communications surveillance, work is also needed on how section 45 is interpreted and applied.

Even though section 45 permits the limitation of the right to privacy, its negative impact on the protection on human rights can be minimised by an interpretation that promotes human rights. This chapter, by applying the lessons learnt in chapters two and three, aims to show that Nigerian courts can play an important role in ensuring that subjects of communications surveillance are not deprived of their human rights. A constitutional amendment of section 45 that provides for better protection for rights may not be feasible in the near future and so the courts must take on the role of interpreting section 45 in a manner that best protects human rights. The thesis takes the position that Nigerian courts have the capacity and duty to balance the need for government-led communications surveillance with the protection of human rights. The adjudication process ought to take the form of a proportionality analysis, involving the adequate protection of human rights while enabling communications surveillance in justifiable circumstances.

A correct interpretation of the limitation clause, however, is only a step towards achieving a communications surveillance regime in Nigeria that protects human rights. The courts also need a strong legal framework for communications surveillance. South Africa, as a foreign jurisdiction in an African context, provides a good example of how a sound communications surveillance law can be used to protect the right to privacy and other rights impacted by communications surveillance at all stages of communications surveillance. The South African courts have also balanced the need for communications surveillance with the protection of human rights as their paramount concern. This approach aligns with the standard in international law.

In order to make recommendations for an appropriate Nigerian framework, in this chapter, the recommendations in chapters two and three are collated and then applied to address the Nigerian problems with communications surveillance, as set out in chapter four. The subsequent discussion proceeds in this order. First, the chapter addresses the manner in which the limitation clause on the right to privacy has been interpreted by the courts and then proposes recommendations for future practice. Thereafter, the discussion makes recommendations for an effective and constitutionally sound law on communications surveillance that adequately protects human rights.

In addition to the proposed interpretation and application of section 45(1), the recommendations are linked to four important themes namely: 1) enacting a comprehensive and primary statute on communications surveillance and other related matters; 2) the development and implementation of sound and fair procedural rules at all stages of communications surveillance; 3) independent and effective oversight mechanisms for communications surveillance; and 4) an effective avenue for redress in cases where communications surveillance is executed unlawfully. Various sub-themes linked to these four pillars are also addressed throughout the chapter. The sub-themes, as summarised in chapter one, encapsulate all the problems in the Nigerian legislative framework that were discussed in chapter four.¹⁰⁹⁷

5.2 The limitation clause must be correctly interpreted and provide a uniform guidance for limiting rights

The reader will recall that section 45(1) of the 1999 Nigerian Constitution provides as follows:

- “(1) Nothing in sections 37 (right to privacy), 38 (freedom of thought, conscience and religion), 39 (freedom of expression), 40 (freedom of assembly and association) and 41(freedom of movement) 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 freedom of other persons”

There are two factors that need to be addressed. These are an interpretation of “reasonably justifiable” that advances human rights and a clear definition of the “legitimate aims” in section 45(1)(a) and (b) of the 1999 Nigerian Constitution. It should be noted that the problem with section 45(1) is an independent problem that is not a prerequisite to the reform of the legislative framework on communications surveillance in Nigeria. However, if section 45 is interpreted to align with the permissible limitation of rights in international law, the rights which can be limited by section 45, which includes the right to privacy, will benefit from dual protection. There is thus a close link between a restrictive interpretation of section 45 and a legislative framework which regulates communication surveillance.

¹⁰⁹⁷ Chapter 1, sec. 1.3.5.3.

5.2.1. An analysis of “reasonably justifiable” for human rights adjudication in Nigeria

The current position that the courts take when interpreting and applying section 45(1) is that laws are usually declared constitutionally valid if they pursue any of the legitimate aims in section 45(1)(a) and (b). There is barely any evaluation of whether the law under review is “reasonably justifiable” as prescribed by section 45(1). This is illustrated by the Supreme Court’s decision in *Asari-Dokubo v Federal Government of Nigeria (FGN)*¹⁰⁹⁸ where it was held that:

“...where National Security is threatened or there is the real likelihood of it being threatened, human rights or the individual rights must be suspended until National Security can be protected or well taken care of”.¹⁰⁹⁹

The decision to refuse the appellant’s bail application was based on whether national security was likely to be jeopardised. No proportionality analysis was conducted between the right to personal liberty and the limitation. The declaration that human rights must be suspended when there is a threat to national security indicates that once there is a legitimate aim for limitation, the right must be limited. Several Nigerian courts have followed this reasoning when adjudicating on cases involving a determination on section 45(1).¹¹⁰⁰

The discussion in chapter four revealed that the Supreme Court’s position in *Asari-Dokubo* is based on an incorrect interpretation of section 45(1).¹¹⁰¹ While it is important for laws to pursue a legitimate aim, section 45 also involves evaluating whether a law limiting rights is “reasonably justifiable in a democratic society”. This means that the court must determine whether the law limiting rights is reasonably justifiable and whether it pursues a legitimate aim. Unfortunately, the reality is that the courts tend to omit the analysis of whether the law is “reasonably justifiable” and reach a decision merely with reference to the issue of whether the law pursues a legitimate aim alone. The second leg of the test is thus overlooked.¹¹⁰²

¹⁰⁹⁸ (2007) LPELR-958 (SC).

¹⁰⁹⁹ (2007) LPELR-958 (SC) 36.

¹¹⁰⁰ *Ibid*; *Williams v Majekodunmi* (1962) 1 All Nigerian Law Report 413; *Federal Republic of Nigeria v Daniel* (2011) LPELR- 4152 (CA) 18; *Hassan v Economic and Financial Crimes Commission* (2013) LPELR-22595 (CA)10; Chapter 4, sec. 4.6.2.

¹¹⁰¹ Chapter 4, sec 4.6.2.

¹¹⁰² There are however a few judicial precedents in Nigeria that depart from this position. One of such is *Inspector General of Police (IGP) v All Nigerian Peoples Party (ANPP)* (2007) LPELR-8217 (CA) 40. This is not to say that there may not be more cases where such an evaluation process

The misinterpretation of section 45(1) could be caused by a lack of understanding of the factors informing the enquiry as to whether a law is “reasonably justifiable”. This is because section 45(1) only states that “nothing” in the listed sections “shall invalidate any law that is reasonably justifiable in a democratic society” and then lists the legitimate aims in sub-sections (a) and (b). This is unfortunate because it should be clear that an analysis of “reasonably justifiable” is also a necessary consideration for determining the constitutional validity of laws that limit rights.

The preferred option is for the 1999 Nigerian Constitution to be amended to reflect specific factors that must be considered when evaluating whether a law is “reasonably justifiable”. An amendment of this sort will provide the courts with precise and clear guidelines on how to conduct the “reasonableness” analysis, as is seen in section 36(1) of the South African Constitution, outlined in chapter three. Section 36(1)(a)-(e) require that laws limiting rights be “reasonable and justifiable” and then provides a list of non-exhaustive factors that must be considered before the limitation of a right may be permitted.

It is, however, accepted that an amendment of the Constitution is not practically likely. The best solution, in the absence of an amendment providing express guidance, is the development of jurisprudence containing sound judicial interpretations of section 45(1) and the introduction of a proportionality analysis in terms of section 45(1). This approach will ensure that laws limiting rights can be adequately tested by the courts and, at the same time, also provide clear guidance to legislative drafters of laws that limit rights. In order to propose recommendations for a better interpretation of section 45, guidance is sought from international law and South Africa for the best interpretation of “reasonably justifiable”.

5.2.1.1 International law standard on defining “reasonable”

The International Covenant on Civil and Political Rights (ICCPR) does not expressly provide that a limitation of rights must be reasonable. Rather, the common language used in the ICCPR is that limitation must be “prescribed by law”, “necessary” and must not be “arbitrary”.¹¹⁰³ These requirements are reflected in articles 17 to 21 of the ICCPR and protect the same rights listed in sections 37 to 41 of the 1999 Nigerian

was used. These could not be located online as this thesis was conducted during the pandemic and in South Africa. Hence, a physical research of print sources was not possible.

¹¹⁰³ Articles 12, 13, 17, 18, 19, 21,

Constitution. The latter provisions are all limited by section 45(1). As discussed in chapter two, the Siracusa Principles have provided very useful guidance for the meaning of the terms “lawful” and “necessary”.¹¹⁰⁴ The interpretation of “arbitrary” was excluded in the Siracusa Principles, but expounded upon in other United Nations documents such as Human Rights Council’s Resolutions, Human Rights Committee’s (HRC) decision and various Special Rapporteur reports.¹¹⁰⁵

According to the Siracusa Principles, a limitation of rights will be “prescribed by law” if such law is of a general application and is reasonable and non-arbitrary.¹¹⁰⁶ Other requirements are: clarity, accessibility and provision of adequate safeguards and effective remedies against abuse.¹¹⁰⁷ This means that one of the components of a reasonable limitation of rights in international law is that the limitation must be “prescribed by law”. For a domestic law to be “prescribed by law”, such law must be reasonable and non-arbitrary.

A reasonable limitation in international law means that a limitation of rights is proportional to the end sought and necessary in any given case.¹¹⁰⁸ “Proportionality” and “necessity” are therefore the tests to determine whether the limitation of rights is “reasonable”.¹¹⁰⁹ Other HRC decisions and General Comments on the limitation of the rights in articles 17-21 also reiterate this definition of “reasonableness”.¹¹¹⁰

¹¹⁰⁴ Siracusa Principles par [B(i) 15-18].

¹¹⁰⁵ Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, OHCHR, A/HRC/13/37 pars [14-19], (28 December 2009) (Martin Scheinin); Special Rapporteur’s report on the promotion and protection of the right to freedom of opinion and expression “surveillance and human rights” A/HRC/ 41/35 (2019) par [24] (Frank La Rue).

¹¹⁰⁶ Siracusa Principles par [B(i) 16].

¹¹⁰⁷ Siracusa Principles par [B(i) 17-18].

¹¹⁰⁸ *Toonen v Australia* Communication No. U.N.Doc. CCPR/C/50/D/488/1992 (1994) par [8.3, 8.6]; *Velichkin v Belarus* Communication No. 1022/2001, U.N Doc. CCPR/C/85/D/1022/2001 (2005) par [7.3]; *Keun-Tae v Republic of Korea*, Communication No.574/1994, CCPR/C/64/D/574/1994; Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 27th session, agenda items 2 and 3, A/HRC/27/37, 30 June 2014, (2014 OHCHR Report), pars [2,6,25]; General Comment 16 par [8].

¹¹⁰⁹ General Comment 31, CCPR/C/21/Rev.1/Add. 13, par [6]; 2014 OHCHR Report pars [22, 23].

¹¹¹⁰ *Velichkin v Belarus* Communication No. 1022/2001, U.N Doc. CCPR/C/85/D/1022/2001 (2005) par [7.3]; *Keun-Tae v Republic of Korea*, Communication No. 574/1994, CCPR/C/64/D/574/1994 (1999) par [12.2]; General Comment No.22: Article 18, CCPR/C/21/Rev.1/Add.4 par [8]; General Comment No.34: Article 19, CCPR/C/21/Rev.1/Add. 4, par [22]; General Comment No.22 par [8]; Article 18; General Comment No.34: Article 19; General Comment 37: Article 21 par [40]; Special Rapporteur’s Report on the promotion and protection of the right to freedom of opinion and expression “surveillance and human rights” A/HRC/ 41/35 (2009) par [24]; 2014 OHCHR Report, pars [2,6,25].

The terms “proportional” and “necessary” are often considered as inseparable. For example, the Siracusa Principles define “necessity” as including proportionality. The other components of “necessity” are that “the limitation must fulfil a pressing public and social need” and “the aim pursued must be aligned with the grounds of limitation in the ICCPR”.¹¹¹¹ The latter components deal with the legitimacy of the aim pursued. This means that the test for “necessity” is proportionality between the limitation and the right, on the one hand, and legitimacy of the aim of the limitation, on the other.

Furthermore, the 2019 Special Rapporteur’s Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression considered “necessary and proportional” as a single component of a three-part test for the limitation of rights.¹¹¹² The Report states that “proportionality” and “necessity” involve an analysis of the connection between the right, the limitation and the aim pursued.¹¹¹³ Also, the means employed must be the least intrusive “among those that might achieve the same protective function”.¹¹¹⁴ The other two components of this three-part test are legality and legitimacy.

The Report of the Special Rapporteur on Human Rights and Fundamental Freedoms while Countering Terrorism (2014 SR Report on Counterterrorism) recommends a four-part proportionality for determining reasonableness.¹¹¹⁵ The four-part test absorbs the “necessity” requirement into a single proportionality test by including a test for the legitimacy of the aim of the limitation.¹¹¹⁶ While this test is tailored specifically for the right to privacy, its elements are the standard factors to be considered when determining whether the limitation of a right is reasonable.¹¹¹⁷ This

¹¹¹¹ Siracusa Principles par [A-10].

¹¹¹² Special Rapporteur’s Report on the promotion and protection of the right to freedom of opinion and expression “surveillance and human rights” A/HRC/ 41/35 (2019) par [24]; General Comment 34 par [34]; General Comment 27 par [14].

¹¹¹³ *Ibid.*

¹¹¹⁴ *Ibid.*

¹¹¹⁵ Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, OHCHR, A/HRC/13/37 par [14-19], (28 December 2009) (Martin Scheinin).

¹¹¹⁶ Siracusa Principles par [A-10].

¹¹¹⁷ General Comment 34 par [34]; General Comment 27 par [14]; American Civil Liberties Union (ACLU) “Privacy in the Digital Age: A Proposal or a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights (March 2014) *Draft Report and General Comment by ACLU* 38.

¹¹¹⁷ Ortino “From ‘non-discrimination’ to ‘reasonableness’: A Paradigm Shift in International Economic Law?” (April 2005) *Jean Monnet Working Paper 01/05 New York University School of Law* 34; Trachtman “Trade and ... Problems, Cost-Benefit Analysis and Subsidiarity” 1998 9 *European Journal of International Law* 33. Grainne de Búrca “The Principle of Proportionality and its

means that when considering whether a limitation is reasonable, the same factors apply when the right to privacy is substituted with the other rights in articles 18-21 of the ICCPR.¹¹¹⁸

The four-part proportionality test entails the following for a limitation of the right to privacy: there be a legitimate aim for the limitation of the right to privacy;¹¹¹⁹ the legitimate aim must be rationally connected to the measure taken to limit the right;¹¹²⁰ the impairment of the right to privacy must be minimal;¹¹²¹ and there must be a fair balance struck between the legitimate aim pursued and the right to privacy.¹¹²² It is therefore recommended, as set out below, that Nigeria adopt the four-part test to interpret the phrase “reasonably justifiable” in section 45(1) when a limitation of rights, including the right to privacy, is considered.

5.2.1.2 African regional law on defining “proportionate” and “necessary”

The discussion in chapter two indicates that the Declaration of Principles on Freedom of Expression and Access to Information (the 2019 Declaration) provides the justification for the limitation of rights in African regional law.¹¹²³ Whilst it is not specifically stated that the justification of limitation of rights is reasonableness, the 2019 Declaration provides that a limitation must be “proportionate” and “necessary”, “prescribed by law” and possess the legitimate aims specified in Principle 9(3) of the 2019 Declaration.

The 2019 Declaration provides further explanation for the terms “proportionate” and “necessary”, “prescribed by law” and “legitimate aims”. The discussion in chapter two also indicates that the 2019 Declaration provides factors for determining whether a limitation of rights is “proportionate” and “necessary”. These factors are a summarised version of the Siracusa Principles. Even though the justification of limitation of rights

Application in the EC Law” 1994 13 *The Yearbook of European Law* (YEL) 113; Jans “Proportionality Revisited” 2000 27 *Legal Issues of Economic Integration* 241.

¹¹¹⁸ Special Rapporteur’s Report on the right to freedom of peaceful assembly and of association A/HRC/26/29 (2014) par [21]; 2014 OHCHR Report par [23].

¹¹¹⁹ American Civil Liberties Union, *Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy Under Article 17 of the International Covenant on Civil and Political Rights* (2014) <https://www.aclu.org/other/human-right-privacy-digital-age> (accessed 2019-06-06) 24.

¹¹²⁰ *Ibid.*

¹¹²¹ *Ibid.*

¹¹²² *Ibid.*

¹¹²³ Adopted by the African Commission on Human and People’s Rights, 65th ordinary session, 21 October to 10 November 2019, Banjul, Gambia.

in the 2019 Declaration relates to the rights to freedom of expression and access to information only, it can be extended to apply to other rights as well because it ultimately reflects the international law standards on limitation of rights.¹¹²⁴

It was concluded in chapter two that international law applies to the interpretation of the limitation clause of the domestic law of Member States of the African Union. However, as discussed in chapter four, the 2019 Declaration is a more practical instrument than the ICCPR to utilise when persuading Nigerian courts to adopt an interpretation of section 45(1) of the 1999 Nigerian Constitution in a manner that aligns with international law. This is because the 2019 Declaration forms part of the African Charter of Human and People's Rights (ACHPR) which has been domesticated in Nigeria.¹¹²⁵

5.2.1.3 South African approach to the limitation of rights

There are some lessons to be learnt from the manner in which the South African constitutional limitation clause reflects the four-part test. This proportionality evaluation, as discussed in chapter three, was instrumental in testing the constitutionality of the Regulation and Provision of Communication Related Information Act (RICA). The application of the test resulted in the Constitutional Court confirming (in part) the High Court's order of invalidity of some of RICA's provisions in *AmaBhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services*.¹¹²⁶ The South African approach to the limitation of rights encapsulates the international law requirements because it includes the proper factors to consider when determining whether a limitation is reasonable. These factors are contained in section 36(1) of the South African Constitution and assist the court to undertake a proportionality analysis.¹¹²⁷ They are also discussed in detail in chapter three.

The factors in section 36(1) reflect the four-part test as follows: The requirements that a fair balance must be struck between the legitimate aim pursued and the limitation to the right to privacy are found in section 36(1)(a) and (c).¹¹²⁸ These factors require an

¹¹²⁴ Principle 9 of the 2019 Declaration of Principle on Freedom of Freedom of Expression.

¹¹²⁵ Chapter 4, sec. 4.4; African Charter on Human and People's Rights (Ratification and Enforcement) Act, Cap A9, LFN 2004.

¹¹²⁶ 2020 (1) SA 90 (GP); 2021 (4) BCLR 349 (CC).

¹¹²⁷ Bilchitz "Privacy, Surveillance and the Duties of Corporations" 2016 TSAR 67.

¹¹²⁸ American Civil Liberties Union, *Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy Under Article 17 of the International Covenant on Civil and*

analysis of the nature of the right and an evaluation of the extent of the limitation.¹¹²⁹ The four-part test requirement that there must be a legitimate aim for the limitation of the right to privacy is mirrored in section 36(1)(b). This examines the importance and purpose of the limitation and the aim which it strives to serve.¹¹³⁰

The requirement in the four-part test that “the legitimate aim must be rationally connected to the measure taken to limit the right” is reflected in section 36(1)(d). This factor considers the “relation between the limitation and its purpose”. Hence, a proportionality analysis between the limitation and the aim pursued is undertaken. The requirement that impairment of the right to privacy must be minimal is reflected in section 36(1)(e). This considers the less restrictive means of achieving the purpose among the options proffered.¹¹³¹ It further evaluates whether the limitation can achieve the aim pursued without being too broad or too inclusive.¹¹³²

The South African legal framework demonstrates that the factors in section 36(1) incorporate the four-part test, encompassing both proportionality and necessity. Whilst it is ideal for a limitation clause to contain a set of listed limitation guidelines, it is not imperative that this be the case. For example, in *S v Makwanyane*, when applying the limitation section in the Interim Constitution (which did not contain the listed factors in section 36), the Constitutional Court adopted good practice by applying a proportionality test even when the Constitution does not specifically require a proportionality test.¹¹³³ The Nigerian courts should emulate this precedent when interpreting section 45(1).

Political Rights (2014) <https://www.aclu.org/other/human-right-privacy-digital-age> (accessed 2019-06-06) 24.

¹¹²⁹ Rautenbach 2005 4 JSAL 632; *S v Bhulwan: S v Gwadiso* 1995 (12) BCLR 1579 (CC) par [18]; *Christian Education SA v Minister of Education* 2000 (10) BCLR 1051 (CC) par [51]; *S v Negal: S v Solberg* 1997 (10) BCLR 1348 (CC) par [168]; Currie and De Waal *The Bill of Rights Handbook* 168.

¹¹³⁰ *Minister of Welfare and Population Development v Fitzpatrick* 2000 (7) BCLR 713 (CC) par [20]; *National Coalition for Gay and Lesbian Equality v Minister of Home Affairs* 2000 (1) BCLR 39 (CC) par [59]; Currie and De Waal *The Bill of Rights Handbook* 164.

¹¹³¹ *Ibid*; Rautenbach 2005 JSAL 634; Currie and De Waal *The Bill of Rights Handbook* 171; Currie and De Waal *The Bill of Rights Handbook* 170.

¹¹³² 2014 OHCHR Report, par [21]; *Law Society of South Africa v Minister for Transport* 2011 (1) SA 400 (CC) par [47]; Rautenbach 2014 PECLR 2232-2234; Andenas and Zleptnig “Proportionality: WTO Law: In Perspective” 2007 42 *Texas International Law Journal* 386; Rautenbach 2005 JSAL 634; Cohen-Eliya and Porat *Proportionality and Constitutional Culture* (2013) 111-113.

¹¹³³ *S v Makwanyane* 1995 (3) SA 391 par [104].

5.2.1.4 Recommendation for Nigeria on interpreting the limitation of rights

The recommended remedy to address the current problem is for the Nigerian courts to apply the four-part proportionality test when interpreting section 45(1). By so doing, Nigerian courts will have to conduct a proportionality analysis to determine whether a limitation is “reasonably justifiable”. This will result in the development of uniform guidelines for section 45(1). The Nigerian Supreme Court should emulate the South African approach, as explained above. The Supreme Court is specifically mentioned here because it is higher in hierarchy than the other courts and all other courts are bound by its decisions.

Uniform precedent will aid legal certainty and provide a detailed and structured framework for balancing the protection of rights and their limitation when necessary. This is not to say that there must be a fixed rule which does not permit any form of flexibility on a case-by-case basis. Flexibility is necessary to avoid harsh outcomes, but a proper framework for such application will provide a yardstick for a detailed proportionality analysis to be conducted in rights’ adjudication involving section 45(1).

The guidelines for interpreting section 45 must ensure the best possible protection of human rights. The end goal should be to protect human rights without hindering the duties of the State when a limitation of rights is necessary and justifiable. This should not become a determination of pitting the protection of the right against permitting the actions of the State, but rather a balance must be struck. The four-part proportionality test provides a clear standard to achieve this balance.

5.2.2 Legitimate aims must be clearly defined in the 1999 Nigerian Constitution

Section 45(1)(a) and (b) of the 1999 Nigerian Constitution list the legitimate aims for the limitation of the right to privacy and other rights. These legitimate aims are defence, public order, public safety, public morals or public health and the protection of the rights and freedom of others. However, the listed aims are not defined in the Constitution. These legitimate aims are also rarely defined when the courts embark on limitation of rights adjudication. As a result, a court seeking to conduct a proportionality analysis to determine whether a limitation is reasonable and justifiable, has little precedent on which to rely when deciding whether a limitation meets a legitimate aim in section 45.

Another effect of the dearth of definitions is that the legitimate aims are utilised broadly by the State and even the legislature to limit human rights. This runs counter to the rule that limitations to rights should be narrowly defined. There is also regular conceptual confusion, with the Nigerian courts interchanging the term “defence” with “national security”.¹¹³⁴ This occurs even though the definitions of these terms are different. It is particularly important during the authorisation of communications surveillance cases that courts do not “stretch” the meaning of national security as this impedes adequate safeguards for human rights.¹¹³⁵

One of the few cases where a legitimate aim is defined is *ANPP v IGP*, where the Court of Appeal defined the terms “public order and “public safety”. This occurred only because the court undertook a proportionality analysis involving the right to freedom of expression and the preservation of public order and public safety. The Court of Appeal had to define the ambit of freedom of expression and the scope of public order and public safety provided in section 45(1)(a) and then declared certain provisions of the Public Order Act (POA) unconstitutional. This is because the POA sought to use the preservation of public order and public safety to stifle the right to demonstrate. It is thus clear that when legitimate aims are defined clearly, an arbitrary interpretation and/or application can be avoided.

The Siracusa Principles, a soft law instrument in International Law, have defined the terms utilised in section 45(1)(a) and (b). These definitions should be adopted as guidelines for defining the terms.

5.2.2.1 International law standard for listing ‘legitimate aims’

One of the fundamental international law requirements for compliant domestic laws that limit human rights is that such laws must be accessible, clear and precise. Section 45(1)(a) and (b) of the 1999 Nigerian Constitution do not align with this requirement. As discussed in chapter four, the legitimate aims in the 1999 Nigerian Constitution overlap to some extent with the limitation clause in the ICCPR and the general

¹¹³⁴ S.1 of the National Security Agencies Act of 1986; *IGP v ANPP*, 39; *Awolowo v Shagari* (1979) 69 SC 51; *Alamiyeseigha v FRN* (2006) 16 NWLR Pt. 1004, 1; *Rabiu v State* (1960) 8 SC 130; *A.G Bendel State v A.G Federation* (1981) 10 SC 1; *Owena v Nigerian Stock Exchange Ltd* (1997) 8 NWLR Pt. 515; *Bronik Motors Ltd v Wema Bank Ltd* (1983) 1 SCNLR 296.

¹¹³⁵ *Christie v United Kingdom*, App. No. 21482/93 (1994) 134; *Al-Nashif v Bulgaria*, App. No. 50963/99, (2002), 124; *Association for European Integration and Human Rights and Ekimdzhev v Bulgaria*, App. No. 62540/00 (2007) par [75].

limitation clause in the UDHR.¹¹³⁶ The legitimate aims for limitation of the rights in section 45(1)(a) and (b) of the 1999 Nigerian Constitution are therefore not problematic in themselves. The problem is a lack of precise definition and consistent application.

The aims listed in the ICCPR are also not defined. It would have been instructive for Nigeria if some of these aims had been expressly defined in the ICCPR or the General Comments published thereunder. The reluctance to provide specific definitions may be as a result of the provisions of the Vienna Convention Law of Treaties (Vienna Convention).¹¹³⁷ Article 2(2) of the Vienna Convention enables Member States to give effect to treaties based on their domestic laws. This approach allows Member States some leeway to apply international law in their domestic context. However, the domestic laws must not be “applied or invoked in a manner that will impair the essence of a Covenant right”.¹¹³⁸

International law permits Member States the flexibility of applying their laws within their specific context.¹¹³⁹ However, this flexibility does not mean that Member States can define the legitimate aims for limitations as they deem fit. The purposes for which rights are limited must be applied so that human rights are protected in the best manner possible. However, in Nigeria, the courts, executive and legislature, apply the legitimate aims in a way that undermines the right in favour of governmental interests. It is therefore necessary to define the legitimate aims in section 45(1)(a) and (b) according to the international law standard to provide better guidance.

The Siracusa Principles, discussed in chapter two, provide definitions (or descriptions) of the frequently used legitimate aims for the limitations of rights in the ICCPR, specifically national security, public health, public order, public safety and public morals.¹¹⁴⁰ Chapter four of the thesis used this interpretation to define the aims listed in the 1999 Nigerian Constitution.¹¹⁴¹ The Siracusa Principles state that a State invoking public morality as a ground for limiting rights “shall demonstrate that the limitation in question is essential to the maintenance of respect for fundamental values

¹¹³⁶ Ugochukwu 2014 *Transnational Human Rights Review* 40. The Nigerian Bill of Rights has its roots in the UDHR; Chapter 4, sec. 4.6.2.

¹¹³⁷ Vienna Convention Law of Treaties, 27 January 1980, United Nations Treaties Series, vol. 1155, 331.

¹¹³⁸ General Comment 31[80] par [6], CCPR/C/21/Rev.1/Add.13.

¹¹³⁹ Article 2(2) Vienna Convention; Bilchitz “Privacy, Surveillance and the Duties of Corporations” 2016 *TSAR* 62.

¹¹⁴⁰ Chapter 2, sec. 2.2.3; Siracusa Principles, par [B (iii-viii) 8-9.

¹¹⁴¹ Chapter 4, sec.4.6.3.

of the community”.¹¹⁴² Also, a threat to public health is described as a situation that demands the “prevention of disease or injury or providing care for the sick”.¹¹⁴³

Protection against a threat to national security is defined as protection of the State “against force or threat of force” to its existence, territorial integrity or political independence.¹¹⁴⁴ Rights will be impaired when Member States do not define a “threat to national security” and when this term is applied too broadly.¹¹⁴⁵ This caution is particularly relevant to communications surveillance which is often undertaken to protect national security.

“Public safety” was defined as “protection against danger to the safety of persons, to their life or physical integrity, or serious damage to property”.¹¹⁴⁶ The definition of public order used in *ANPP v IGP* is similar to the definition of public safety in the Siracusa Principles.¹¹⁴⁷ These aims therefore operate hand-in-hand because if public order is threatened, so is public safety.

The definition of the legitimate aims in the Siracusa Principles is therefore useful for Nigeria as this is the basis upon which a limitation will be justifiable. Also, an effective proportionality analysis cannot be undertaken in human rights adjudication without ascertaining the scope of the legitimate aim. The definitions in the Siracusa Principles should therefore be adopted into the Constitution or by the courts when interpreting section 45(1)(a) and (b).

5.2.2.2 South African approach for listing ‘legitimate aims’

The South African Constitution does not provide for specific legitimate aims justifying the limitation of rights in its general limitation clause, section 36. Nevertheless, judicial precedent demonstrates that laws must have a legitimate purpose - as is required by the section 36(1)(b) factor, namely the purpose of the limitation.¹¹⁴⁸

¹¹⁴² Siracusa Principles, Siracusa Principles par [B(v) 25] 8.

¹¹⁴³ Siracusa Principles, par [B(iv) 25] 8; Chapter 4, sec.4.6.3.3.

¹¹⁴⁴ Siracusa Principles, pars [B(vi) 29-32] 8-9.

¹¹⁴⁵ *Manohar v Union of India*, Supreme Court of India, Writ Petition (Criminal) No. 314 of 2021, 27 October 2021 file:///Users/tope/Downloads/Manohar_Lal_Sharma_vs_Union_Of_India_on_27_October_2021.PDF (accessed on 2022-01-03); *Klass v Germany* par [45-46]; 2014 OHCHR Report, pars [23-25].

¹¹⁴⁶ Siracusa Principles Document, pars [33 & 34] 9.

¹¹⁴⁷ *IGP v ANPP*, 39.

¹¹⁴⁸ Chapter 3, sec. 3.6.3.3; S.16(5)(a) of 70 of 2002 provides for the purposes for the execution of communications surveillance in Nigeria; *Minister of Welfare and Population Development v Fitzpatrick* 2000 (7) BCLR 713 (CC) par [20]; *National Coalition for Gay and Lesbian Equality v*

The constitutional validity of laws in South Africa that limit rights is tested against an evaluation of whether the limitation of the right is proportional to the legitimate aim.¹¹⁴⁹ This is different from the Nigerian approach that already has a list of legitimate aims. Although there is no umbrella definition of legitimate aims in section 36, Nigeria can still benefit from South Africa's overall approach to the proportionality exercise. Chapters three and four and the argument above strongly recommend that Nigeria include in its proportionality evaluation an analysis of the relationship between the limitation and the aim the limitation strives to achieve. This approach aligns with the standard in international law. Nigeria, however, also requires a definition of the specific legitimate aims provided by her Constitution in order to apply the South African approach in the Nigerian context appropriately.

5.2.2.3 Recommendations for listing 'legitimate aims'

The Siracusa Principles provide specific definitions of the aims for limiting the right to privacy. These definitions should be adopted in Nigeria. It would also be worthwhile expanding section 318 of the 1999 Nigerian Constitution that deals with interpretation of terms to include these definitions.¹¹⁵⁰

Constitutional amendment is a long process and may not be an immediate solution for Nigeria. It is more practical for the courts to refer to the Siracusa Principles during human rights adjudication in order to define the legitimate aims. The Courts cannot, however, do so directly because the ICCPR has not been domesticated in Nigeria. Nonetheless, the preamble to the Fundamental Rights (Enforcement Procedure) Rules (FREPR), discussed in chapter four, permits courts to consider international law when adjudicating human rights cases.¹¹⁵¹ The courts can therefore rely on the FREPR to utilise the Siracusa Principles definitions when defining the legitimate aims in section 45 and in this way set new precedent that develops the law appropriately and creates legal certainty.

Minister of Home Affairs 2000 (1) BCLR 39 (CC) par [59]; Currie and De Waal *The Bill of Rights Handbook* 3ed (2013) 164.

¹¹⁴⁹ S.36(1)(b), (d) and (e) of the South African Constitution.

¹¹⁵⁰ S.318 of the 1999 Nigerian Constitution defines the terms used in the Constitution. For example, terms like "House of Assembly", "Federation" "Law" and "Statutes" are interpreted. It should be expanded to include the terms, like "national security", "defence", "public health", public safety and "public order" used in section 45.

¹¹⁵¹ Chapter 4, sec.4.2; Preamble 3 of the FREPR.

5.3 A comprehensive statute on communications surveillance in Nigeria

The laws regulating communications surveillance in Nigeria are the Terrorism Prevention and Prohibition Act, 2022 (TPPA), the Cybercrimes (Prevention, Prohibition etc) Act, 2015 (CPPA), the Nigerian Communications Act, 2003 (NCA) and the Lawful Interception of Communications Regulation, 2019 (LICR). The NCA is the empowering statute of the LICR. The objective of the CPPA and the TPPA is to facilitate the criminal justice procedure for cybercrimes and terrorism respectively. Thus, the provisions on communications surveillance in the CPPA and the TPPA are merely consequential to their aims. The LICR, however, is focused on regulating communications surveillance in Nigeria, but is lower in status to the TPPA, NCA and the CPPA.

The different provisions on communications surveillance in these laws cause several problems, which are discussed in the next sub-section. **In brief, the issues are lack of clarity on the laws regulating communications surveillance (this issue includes conflicting provisions on communications surveillance and lack of foreseeability of the laws),** accessibility of the LICR, overreach of the laws and lack of safeguards for the acquisition of metadata. The discussion in the subsequent sub-section highlights the problems and provide recommendations from international and regional laws as well as the South African legal framework on communications surveillance.

5.3.1 Lack of clarity of laws regulating communications surveillance

5.3.1.1 Conflicting provisions in the laws

There are conflicting provisions in the Nigerian laws regulating communications surveillance. Read together, the result is uncertainty regarding the applicable authorising body for a communications surveillance order, the procedure for granting a surveillance warrant and the nature of the crime that can prompt surveillance. As discussed in chapter two, international law stipulates that these matters must be clearly defined for a communications surveillance law to be regarded as lawful and non-arbitrary. The conflicting provisions in the law are now set out explicitly, starting with the NCA and the LICR.

Section 146(2) of the NCA conflicts with Regulations 4 and 23 of the LICR. The NCA, on the one hand, provides that any authority, that is any organ of State, can intercept any electronic communication in Nigeria and communications service providers

(CSPs) must provide access to their networks. The LICR, on the other hand, contains a list of parastatals, mostly law enforcement agencies (LEAs), that can be permitted to intercept communications. Even though the LICR provides more protection for the right to privacy by specifying the authorised person to intercept communications, the NCA still supersedes the LICR. This is because the NCA, being a statute, is a superior law and it is also the empowering law for the LICR. When the laws are read together, it is unclear whether only LEAs or all government agencies are permitted to intercept communications.

The LICR also has conflicting definitions of which agencies are authorised to intercept communications. Regulation 23 defines “authorised agency” as the Office of the National Security Adviser, the State Security Service and the Nigeria Police Force. Meanwhile “authorised agencies” in the exact same provision, that is Regulation 23, is defined more broadly as:

“Nigeria Police Force, National Intelligence Agency, State Security Services, Economic and Financial Crimes Commission, National Drug Law Enforcement Agency and any other organization or agency as the Commission may from time to time specify and publish”.

The result of these conflicting provisions is that the law lacks clarity. In addition, the inferior status of the law renders it ineffective as the primary law on communications surveillance in Nigeria. Clearly, the hierarchy of the relevant laws must be rectified.

Another conflict is between section 45 of the CPPA and Regulation 13(3) of the LICR, that provides procedural guidelines for the application of an interception order. On the one hand, section 45 provides that an applicant for an interception order must satisfy the court that there are reasonable grounds to believe that communications surveillance is required for the criminal justice procedure relating to cybercrimes.¹¹⁵² There are no specific provisions expounding on what the “reasonable grounds” could be - hence the problem of abstractness. As a result, section 45 lacks clarity and precision.¹¹⁵³

Regulation 13(3) of the LICR, on the other hand, provides that a judge can only grant an interception order if the facts alleged in the application are “reasonable and

¹¹⁵² S.45(3)(a)-(d) of the CPPA.

¹¹⁵³ This is not the only problem with s.45, but the focus here is the confusion with the procedural guidelines between the laws. The effect of the abstract procedural guidelines on the protection of the right to privacy is discussed in section 5.4 below, where the need for an effective procedural guideline is recommended.

persuasive enough to believe” that the legitimate aims for which communication surveillance can be granted has occurred. These “legitimate aims” are listed in Regulation 7 of the LICR. There are no further practical guidelines as to what is considered “reasonable” and “persuasive”. The TPPA also provides no judicial guidelines for an application for an interception order. The conflicting provisions procedural guidelines in the CPPA and LICR for an application of an interception order create confusion.

The conflict occurs when a person is suspected of multiple crimes and all the laws apply to the scenario. Will the application for an interception order be brought pursuant to the CPPA, the LICR or TPPA? Will the presiding judge choose the ground requiring “reasonableness” in the CPPA or the “reasonable and persuasive” ground in the LICR? This confusion is compounded by the conflicting provisions on the mode of the supporting information needed for the application. Section 39 of the CPPA provides that the application for an interception order must be accompanied by information on oath. The TPPA does not require that information be provided under oath.

Furthermore, the nature of the crime that can result in communications surveillance is not sufficiently clear. Although the CPPA and LICR stipulate that communications surveillance can be used for the criminal justice procedure regarding all crimes, the procedural guideline of the former suggests that it should be for cybercrimes alone. The LICR provides that communications surveillance can be used for all crimes, but has an unclear and undefined list of other aims such as “interest of national interest, public emergency and safety”, protection of economic wellbeing”.¹¹⁵⁴ These aims lack clarity.

5.3.1.2 The problem of foreseeability

The laws also lack foreseeability because the legitimate aims for which communications surveillance is permitted is very broad. Foreseeability in the context of communications surveillance means that the law “must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measure.”¹¹⁵⁵ In other

¹¹⁵⁴ Regulation 7 of the LICR.

¹¹⁵⁵ The latter refers to the procedural guideline in the laws regulating communications surveillance and this is discussed in section 5.4 below. *Zakharov v Russia* v par [229]; *Malone v United Kingdom* par [67]; *Leander v Sweden*, App. No. 9248/81 (1987) par [51]; *Huvig v France*, Series A, No.176-B, (1990) par [29]; *Valenzuela Contreras v Spain*, 58/1997/842/1048(1998) par [46];

words, the laws do not state precisely which situations may prompt communications surveillance. The CPPA and the LICR provide that a person suspected of a crime may be subject to communications surveillance. However, they do not state precisely what types of offences will prompt surveillance.

In addition to communication surveillance being utilised for all crimes, the LICR also permits other circumstances for the use of communications surveillance. These are “interest of national security”, “protecting and safeguarding the economic wellbeing of Nigerians”, “in the interest of public emergency or safety” and “giving effect to any international mutual agreements, which Nigeria is a party”.¹¹⁵⁶ The LICR does not specify the circumstance that constitute “interest of national security” or “economic wellbeing of Nigerians”. “Public emergency and safety” are not vague when defined in light of the Siracusa Principles as discussed in section 5.2.2 above. Otherwise, “public emergency and safety” remains vague and problematic in the context of foreseeability of communications surveillance law.

The TPPA seems to be foreseeable because the provision regarding communications surveillance relates to the offence of terrorism only, unlike the CPPA and the LICR that do not specify the offences. However, the TPPA lacks foreseeability as the circumstances for determining whether a person should be subjected to surveillance are vague. Section 29(1) of the TPPA provides that communications surveillance may be executed for “the purpose of the prevention of terrorist acts or to enhance the detection of offences related to the preparation of a terrorist act or the prosecution of offences in this Act ...” The prevention of terrorist acts falls under the broad category of criminal justice procedure and is clear. However, the TPPA does not provide any scope or manner for which communications surveillance may be used to enhance the detection of terrorist activities and therefore unforeseeable. The exact activities that will subject a person to surveillance in this regard are unclear, with the result that the TPPA is not foreseeable.

Rotaru v Romania, [GC], no. 28341/95, (2000) par [55]; *Weber and Saravia v Germany*, App. no. 54934/00 (2006) par [93]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [75].

¹¹⁵⁶ Regulation 7(3)(a)-(e) of the LICR.

These conflicting provisions create confusion, are vague and are also difficult to implement. The lack of foreseeability of the laws also provides public authorities with unfettered powers. Reform is therefore needed.

5.3.1.3 International law standard for regulating clear domestic laws on communications surveillance

This section draws on the discussion in chapter two regarding the international law standard on the restriction of the right to privacy. The international standards discussed in chapter two will guide the recommendation for reforms in this section.

Article 17 of the ICCPR protects the right to privacy of communications and correspondence.¹¹⁵⁷ In chapter two it was shown that the international law requirement for protection of privacy involves Member States ensuring that people's communications and correspondence must be "delivered to the address without interception and without being opened or otherwise read".¹¹⁵⁸ Communications surveillance interferes with the right to privacy of communications and correspondence and must be executed lawfully and in a manner that is non-arbitrary. Although the right to privacy is not absolute, its limitation must be lawful and non-arbitrary.

Lawfulness and non-arbitrariness comprise a single component that requires any limitation on the right to privacy to be backed by a law that is reasonable.¹¹⁵⁹ In section 5.2.2 above, it was shown that a reasonable limitation of rights in terms of international law refers to proportionality to the aim pursued and necessity in the circumstances. The discussion in chapter two identified broad guidelines in international law for the limitation of the right to privacy. Domestic laws regulating communications surveillance will only be deemed reasonable if they accord with these guidelines. The guidelines include the law being "publicly accessible, clear, precise, comprehensive and non-discriminatory".¹¹⁶⁰ The law must also be reasonable and specify in detail the specific circumstances in which interference is permitted.¹¹⁶¹

¹¹⁵⁷ Article 17 of the ICCPR.

¹¹⁵⁸ General Comment 16 par [8]; Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40), annex VI, par [8].

¹¹⁵⁹ 2014 OHCHR Report, par [21].

¹¹⁶⁰ General Comment 16 par [4]; *Hulst v Netherland*, Communication No. U.N.Doc. CCPR/C/82/D/903/1999 (2004) par [7.7].

¹¹⁶¹ Report of the United Nation High Commissioner for Human Rights "The Right to Privacy in the Digital Age" (3 August 2018) A/HRC/39/29 (2018 report) par [10].

International law also requires that laws regulating communications surveillance must be foreseeable. The concept of foreseeability of laws in the surveillance context, however, is not expounded upon. It seems that the concept of foreseeability of surveillance was adopted from the European regional law. The ECtHR has addressed it in detail (see the discussion in section 5.3.1.2. below). This signifies the influence of European regional law, as the leading jurisprudence for regulating communications surveillance law. Thus, most of the specific recommendations for Nigeria's communications surveillance regulation reforms will be drawn from the decisions of European regional courts. This is also because the European regional courts, unlike the Human Rights Committee, have tested many European laws and developed a minimum standard that ensures human rights are adequately protected during surveillance.

5.3.1.4. Regional law standards for regulating clear domestic laws on communications surveillance

Both the African and European regional law provide solutions for reform in Nigeria. African regional law provides guidelines for communications surveillance through the Declaration of Principles on Freedom of Expression and Access to Information (the 2019 Declaration).¹¹⁶² The African Court on Human Rights (ACtHR) has not had the opportunity to preside on cases relating to communications surveillance. The broad guidelines formulated from ACHPR on the limitation of rights do not provide precise and specific solutions. In principle, the broad guidelines for regulating communications surveillance in international law, African and European regional laws are similar. They all require that laws regulating communications surveillance must be “prescribed by law”, “serve a legitimate” and be “reasonable (necessary and proportionate).”¹¹⁶³ As a result, the relevant African regional law requirement on communications surveillance will be highlighted. However, the application of those broad guidelines to practical laws will be drawn from the European Regional law.

¹¹⁶² Adopted by the African Commission on Human and People's Rights, 65th ordinary session, 21 October to 10 November 2019, Banjul, Gambia.

¹¹⁶³ Report of the United Nation High Commissioner for Human Rights “The Right to Privacy in the Digital Age” (3 August 2018) A/HRC/39/29 (2018 report) par [10]; General Comment 16 par [4]; *Hulst v Netherland*, Communication No. U.N.Doc. CCPR/C/82/D/903/1999 (2004) par [7.7]; Principle 9 of the 2019 Declaration of Principles on Freedom of Expression and Access to Information; *Zakharov v Russia* App. No. 47143/06, (2015) par [227]; *Kennedy v United Kingdom*, No. 26839/05 (18 May 2010) par [130].

The European regional courts developed guidelines for laws regulating communications surveillance when it tested various laws of the Contracting States of the Charter of Fundamental Rights of the European Union (EU Charter) and the European Convention on Human Rights. The jurisprudence of the European Court of Human Rights (ECtHR) focuses on communications surveillance, while the Court of Justice of the European Union (CJEU) focuses on the data privacy.¹¹⁶⁴ Consequently, the ECtHR's decisions are more beneficial for Nigeria to the aim of this thesis and will be relied on in this chapter. However, as the African regional law is also useful, it will be addressed first.

5.3.1.4.1. African regional law standard for regulating clear domestic laws on communications surveillance

Regulation 41(2) of the 2019 Declaration provides that:

“States shall only engage in targeted communications surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.”

The above provisions indicate that the domestic laws of Member States regulating communications surveillance must conform with international law. This is a good provision for Nigeria on which to rely, in order to persuade the courts to consider international law in its decisions relating to communications surveillance. As highlighted in chapter four, Nigeria has not domesticated the ICCPR and other international human rights treaties. As a result, these treaties do not bind the judiciary or legislature.

The provision in the 2019 Declaration mandates Member States to ensure that their laws reflect international law standards. Nigeria must therefore ensure that her laws on communications surveillance align with international human rights law. This means that laws regulating communications surveillance must be “publicly accessible, clear, precise, comprehensive and non-discriminatory” as required by international law.¹¹⁶⁵

¹¹⁶⁴ Chapter 2, sec. 2.5; Fabbrini “Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States” 2015 28 *Harvard Human Rights Journal* 69; Newell “The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S and Europe” 2014 10 *Journal of Law and Policy* 494.

¹¹⁶⁵ General Comment 16 par [4]; *Hulst v Netherland*, Communication No. U.N.Doc. CCPR/C/82/D/903/1999 (2004) par [7.7].

Principle 41(2) also specifies that communications surveillance must be executed only when there is a reasonable suspicion that a serious crime has been committed. This signifies the ground on which the facts supporting the application for a communications surveillance order will be evaluated. When compared to the ground in the LICR and CPPA, a “reasonable suspicion of an offence” is a more specific ground for evaluating whether a communications surveillance order should be granted.

Although, the ground for granting a surveillance order applies to only offences in the 2019 Declaration, there are other legitimate grounds for communications surveillance. It can however be deduced that the “reasonable suspicion of an offence” is an example of what is required from Member States. Hence, Nigeria can adopt the ground for granting a surveillance order in the 2019 Declaration, that is “reasonable suspicion” into the proposed statute.

5.3.1.4.2 European regional law standard for regulating clear domestic laws on communications surveillance

Chapter two identified the broad guidelines in international laws provided for laws interfering with privacy.¹¹⁶⁶ These are also highlighted in 5.2.1.2 above. Similarly, article 8(2) of the ECHR provides a broad guideline for the limitation of the right to privacy and by stating that interference with the right to privacy must be “in accordance with the law”, “necessary in a democratic society” and be for a legitimate purpose.¹¹⁶⁷ However, both Member States of the international and European regional human rights treaties have interpreted these broad guidelines in relation to communications surveillance in a manner that inadequately safeguards human rights.

The European Court of Human Rights (ECtHR) has also developed minimum safeguards that must be provided in laws regulating communications surveillance. These were discussed in chapter two and in this chapter will be applied to recommend a comprehensive law for Nigeria. These minimum safeguards embody international and European regional law’s broad guidelines for laws limiting the right to privacy and unlike the broad guidelines, provide specific provisions that must be included in communications surveillance laws. They are not rigid and each Contracting State may

¹¹⁶⁶ This is also indicated section 5.2.1.2 above.

¹¹⁶⁷ *Association for European Integration and Human Rights and Ekimdzhiiev v Bulgaria* par [70].

apply them to fit their domestic context.¹¹⁶⁸ The ECtHR's minimum safeguard requires clarity and foreseeability of the laws regulating communications surveillance of Contracting States.¹¹⁶⁹

The ECtHR's incorporated the foreseeability requirements in its minimum safeguards developed for communications surveillance as follows:

“the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped;”¹¹⁷⁰

The nature of offences refers to the specific offences that can prompt surveillance and must be specifically defined in the State's legal framework. This means that there must be sufficient detail about the nature of offences that can prompt surveillance. Simply stating that all crimes can prompt surveillance is vague and renders the law unforeseeable. In *Zakhorov v Russia*, the ECtHR held that the Russian law on surveillance permitting interception of communication for offences with a maximum penalty of more than three years and above is clear enough.¹¹⁷¹ This dictum will form the basis for the recommendation of the proposed Nigerian law on communications surveillance.

Another aspect of foreseeability is that the law must determine the activities relating to a person that may prompt surveillance, that is, whether the person is suspected of, accused of, or possesses information about the offence. The ECtHR held that surveillance in respect of persons who may have information about an offence, is justifiable. However, there must be legislation or established case-law that defines what it means for a person to have information about an offence. Otherwise, the law is not foreseeable.¹¹⁷² This decision will also be recommended for Nigeria's new law and discussed further in 5.3.1.4.

¹¹⁶⁸ *Zakharov v Russia*, App. No. 47143/06, (2015) par [171]; *Kennedy v United Kingdom*, App. No. 26839/05 (18 May 2010) par [124]; Chapter 2, sec. 2.5.1.1 In chapter two it was shown that the ECtHR declared that a domestic law providing an effective avenue for redress may be absolved from a claim for a possible unjustifiable surveillance *in abstracto* unless claimants prove the existence of a personal situation that may cause victimisation. This indicates that Contracting States have the flexibility of determining the measures they will provide to safeguard rights in their surveillance regime. The measures must however align with the ECtHR's minimum requirements. The oversight mechanisms in the German and Russian jurisprudence on surveillance are discussed in section 5.5 below.

¹¹⁶⁹ *Zakharov v Russia* par [236].

¹¹⁷⁰ *Ibid.*

¹¹⁷¹ *Zakharov v Russia* par [244]; *Kennedy v United Kingdom* par [159]; *Iordachi v Moldova* 25198/02 (10 February 2009) pars [43-44].

¹¹⁷² *Zakharov v Russia* par [245].

5.3.1.5 South African approach to regulating clear laws on communications surveillance

The RICA is the primary statute regulating communications surveillance in South Africa. Other statutes, like the Criminal Procedure Act¹¹⁷³ and the Correctional Services Act,¹¹⁷⁴ also provide for communications surveillance in relation to their peculiar functions. These functions include criminal justice procedures.¹¹⁷⁵ Chapter three discussed many of the good examples for Nigeria to follow, but also highlighted the problems with the South African communications surveillance regulation regime. It concluded that the RICA does not adequately safeguard human rights when regulating communications surveillance. However, South Africa's communications surveillance laws provide better safeguards for human rights than their Nigerian counterparts do. Unlike Nigeria's regime that requires a complete overhaul, the RICA only needs an amendment to rectify identified loopholes.

The RICA is comparatively useful because its provisions setting out the procedural guidelines for the application of an interception order are clear and transparent. For example, the RICA not only defines the authorised persons who may apply for an interception order, but also specifies the type of information that can be obtained based on the functions of the agency.¹¹⁷⁶ This provision also guides the presiding judge to hold the LEAs accountable, because they can only apply for information that is necessary for the investigation within their units.

Nigeria can learn from the clarity of the terms and the structural composition of the RICA. Section 1 of the RICA, the definition section, is especially detailed. The clarity of the definition of a designated judge, in particular, enabled the Constitutional Court in *AmaBhungane* to read-in an implied power of the Minister of Justice to appoint a designated judge.¹¹⁷⁷ If an alternative decision was reached, namely that the Minister

¹¹⁷³ The Criminal Procedure Act 51 of 1977.

¹¹⁷⁴ The Correctional Services Act 111 of 1998.

¹¹⁷⁵ S.1 of 111 of 1998; S.205 of 51 of 1977.

¹¹⁷⁶ S.1 and 16(3) of 70 of 2002.

¹¹⁷⁷ S.1 of 70 of 2002 defines a designated judge as "any judge of a High Court discharged from active service under section 3(2) of the Judge's Remuneration and Conditions of Employment (Act No.47 of 2001), or any retired judge, who is designated by the Minister to perform the functions of a designated judge for purposes of this Act."

of Justice lacked the power to designate a judge, the RICA would have been “bereft of meaningful operability.”¹¹⁷⁸

Another positive aspect of the RICA is that it is higher in the hierarchy of laws when compared to other statutes which permit communications surveillance in South Africa. Section 2 of the RICA states clearly that communications surveillance is unlawful except if it is executed in terms of the Act. Hence, other statutes providing for communications surveillance must be empowered by the RICA to provide regulation in this respect and this system ensures uniformity of laws. This resolves the issue of hierarchy of the laws in the South African surveillance regulation regime. It is recommended that Nigeria should emulate this approach to the extent that RICA is the primary law. However, a stronger hierarchy that enables other laws to refer to the proposed statute on communications surveillance for procedural guideline is needed in Nigeria. One of the loopholes in the RICA is that it permits other laws to provide different procedural guideline for communications surveillance which may not provide the same safeguards for rights. This causes conflict and an avenue for LEAs to bypass the safeguards in the RICA.

Section 9 of the RICA empowers the legislature to formulate regulations in terms of the Correctional Services Act for communications surveillance that will be executed in prisons.¹¹⁷⁹ This means that the communications surveillance regulation applicable in prisons is different from the RICA and does not protect privacy as well as the RICA.¹¹⁸⁰ Section 15 of the RICA permits other laws to provide procedures for the acquisition of metadata.¹¹⁸¹ Provisions like section 9 and 15 of the RICA must therefore be avoided in the new Nigerian law. Rather, there must be a specific provision stating that other laws regulating communications surveillance in Nigeria must utilise the procedural guideline in the new law.¹¹⁸² This kind of specific provision will enable other statutes

¹¹⁷⁸ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* (CC) par [79].

¹¹⁷⁹ S.9 of 70 of 2002.

¹¹⁸⁰ Also, s.9 of the RICA violates the international law standard requiring the accessibility of laws limiting the right to privacy. This problem is discussed in detail in sub-section 5.3.2 below. The Regulations formulated under the Correctional Services Act for communications surveillance in prisons must however still be submitted to parliament. It is hoped that parliament ensures that the Regulations are on par with the RICA.

¹¹⁸¹ S.15(1) of 2002.

¹¹⁸² If is necessary to formulate a regulation to provide for certain matters that are not covered by the statute or which are industry-specific, the subordinate nature of such other laws must be stated in the proposed statute. Such subordinate law must also be approved by parliament to provide an oversight function that will ensure that the law does not provide overbroad powers to execute

requiring communications surveillance to refer to and apply the proposed statute when their objectives require communications surveillance.

Regarding foreseeability of the RICA, the provisions of section 16(5)(a) are sufficiently clear and enables a person to know the circumstances in which they may be subject to surveillance. The Schedule to the RICA provides for offences that can prompt communications surveillance hence it defines the term “serious crime”.¹¹⁸³ As discussed in chapter four, Nigeria and South Africa have a history of oppression. In the light of these countries’ past histories, it is important to both countries that the State does not possess wide discretionary powers in respect of communications surveillance that can be used to erode democracy and oppress opponents. The inclusion of a list of offences that can prompt communications surveillance ensures that neither the courts nor LEAs have to determine what offences qualify as serious. Nigeria should adopt the South African approach and limit communications surveillance to the same offences listed in the Schedule to the RICA.

The other legitimate aims namely “an actual (or potential) threat to the public health or safety, national security...” and “compelling national economic interest” are not defined in the RICA. However, qualifying words like “compelling” and “actual” signify that the designated judge must be convinced that there are aggravating circumstances that can result in the use of communications surveillance. Thus, communications surveillance in South Africa is not used in the ordinary course of criminal justice procedure, but for serious cases.¹¹⁸⁴ The South African approach aligns with the international standard. Nigeria should adopt this approach by qualifying the legitimate aims for regulating communications surveillance to indicate that communications surveillance should be utilised in aggravating circumstances only.

Regarding definitions of the legitimate aims, serious crime excluded, the lack of definitions of these legitimate aims for communications surveillance listed in section 16(5) of the RICA does mean that the RICA is not foreseeable. Bearing in mind the

communications surveillance to the State. This will ensure that the law aligns with the provisions in the proposed statute.

¹¹⁸³ *AmaBhungane v Minister of Justice* par [27] {*AmaBhungane v Minister of Justice (GP)*}; The offences in the Schedule to the RICA include high treason, terrorism, and sabotage and “any offence which could result in the loss of a person’s life or serious risk of loss of a person’s life.”

¹¹⁸⁴ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services (CC)* par [30].

ECtHR's judgment that the holistic jurisprudence of a State must be considered to determine foreseeability,¹¹⁸⁵ the RICA is arguably foreseeable.

The discussion in chapter four and section 5.2.2 above indicates that Nigeria does not define terms in its constitutional limitation clause (section 45 of the 1999 Constitution). The Nigerian case-law also has a scarcity of a proportionality evaluation jurisprudence in its section 45 adjudication, coupled with a failure to engage on the legitimate aims for the limitation of rights.¹¹⁸⁶ A proportionality exercise involves interpreting the scope of the right in issue and the definition of the aim pursued.

To ensure foreseeability, the constitutional legitimate aims which are recommended for communications surveillance in Nigeria, that is "threat to national security", preservation of public health, order or safety should be defined in the statute regulating communication surveillance. The definitions for these terms as adopted from the Siracusa Principles have already been set out in chapter four and section 5.2.2 above. The qualifying words "actual" or "potential" should be added to "threat to national security" so that the law enforcement officers (LEOs) have an additional burden to prove that the threat has occurred, is occurring or the potential of it occurring.

5.3.1.6 Recommendations for regulating a clear law on communications surveillance in Nigeria

The problem with conflicting communications surveillance laws is a lack of clarity and precision. The solution to this is an enactment of a new primary statute that provides a comprehensive procedure for all stages of communications surveillance. The new statute must also adequately balance the right to privacy with the State's interest in obtaining information. The statute must repeal the existing provisions on communications surveillance in other laws. Where other laws, such as the TPPA and the CPPA, list communications surveillance in the pursuance of their aims, they must be amended to refer to the proposed statute to utilise surveillance.

The emphasis on the law being a statute (as opposed to a subordinate regulation) is because it is the only form of law that can effectively repeal the provisions on communications surveillance in the TPPA, the CPPA and the NCA. The LICR will also become redundant once its enabling provisions in the NCA is repealed. This means

¹¹⁸⁵ *Zakharov v Russia* par [245].

¹¹⁸⁶ This is discussed in detail in section 5.2.2 above.

that the proposed statute must specifically disempower the NCA and, by extension, the Nigerian Communications Commission (NCC) from making any provisions or implementing any actions regarding communications surveillance in Nigeria. Section 5.3.3 discusses the problem of overreach of laws in the LICR, which affects the CPPA as well. When there is a single statute regulating communications surveillance, the problem posed in 5.3.1.1 above concerning the law that will apply where a suspect is charged with multiple counts, will not occur. This is because only the proposed statute will regulate communications surveillance.

The Nigerian Criminal Code classifies offences into felony, misdemeanour or simple offences, according to the severity of their punishment.¹¹⁸⁷ Felonies are offences punishable with an imprisonment of three years and above.¹¹⁸⁸ Thus, the proposed statute should not permit communications surveillance for criminal justice procedures for simple offences and misdemeanours as they are not serious offences. However, there are many offences that qualify as felonies and this may leave a wide discretionary power for the State and enable LEAs to use communications surveillance when it is not necessary. The South African approach which provides a list of offences that can prompt communications surveillance in the Schedule to the RICA is therefore preferred and hereby recommended.¹¹⁸⁹

It is also recommended that “threat to national security” “public emergency and public safety” should be defined by including a section for definition of terms using the Siracusa Principles as a guide to the definition. The legitimate aims for implementing communications surveillance should also include preservation of public health and public order as well. The 1999 Nigerian Constitution permits the limitation of the right to privacy for these aims. A “threat to national security” should also be qualified with

¹¹⁸⁷ S.6 of the Nigerian Criminal Code Act Cap C38 of the Laws of Federation of Nigeria 2004 provides for three categories of offences. They are simple offences, misdemeanours and felonies. Simple offences and misdemeanours are offences punishable with an imprisonment of less than six months or less than three years respectively. Felonies are punishable with an imprisonment of three years or more.

¹¹⁸⁸ *Ibid.*

¹¹⁸⁹ These offences include high treason, any offence relating to terrorism, any offence involving sabotage, sedition, any offence that could result in the loss of a person’s life or serious risk of loss of life, racketeering, criminal gang activities, dealing in drugs, dealing in or smuggling of ammunition, firearms, explosives or armament, any offence the punishment whereof may be imprisonment for life or a period of imprisonment exceeding five years without an option of fine. Also, the offences referred to in articles 6, 7 and 8 of Rome Statute of the International Criminal Court.

“actual” and “potential” in order to guide the courts that concrete evidence indicating an aggravating circumstance is required. This will ensure legal certainty and clarity.

It is further recommended that the offences listed in the RICA should be adopted as the list of offences that can prompt communications surveillance. Also, communications surveillance should be evaluated based on whether there is a reasonable suspicion that the circumstances underlying the legitimate aim is occurring or has occurred. Grounds like “reasonable and persuasive enough to believe” that the legitimate aim occurred should not be used.

5.3.2 Lack of accessibility of the laws – public participation in law-making

The way in which the LICR is formulated and was passed are the main accessibility problems. The LICR is a regulation which was formulated by the NCC and was not subject to parliamentary debate and public opinion, as would have been the case if it had been a statute. As discussed in chapter four, there is no uniform procedure for the promulgation and formulation of subordinate laws in Nigeria.¹¹⁹⁰ This means that the requirement of public participation (or accessibility as it is known in international law) for the enactment of statute does not occur when a regulation becomes law. Public participation only occurs when specifically mandated by the enabling statute. The NCA, however, as the enabling statute for the LICR does not provide for public participation or consultation with the public as a prerequisite for the formulation and implementation of its subordinate laws.

Before the implementation of the LICR in 2019, a draft regulation prepared in 2014 under the NCA also provided for interception warrants.¹¹⁹¹ The draft 2014 regulation and the eventually formulated 2019 LICR are substantially similar, but in the latter the express provision that an interception warrant must be authorised by a judge is deleted. The result is an increased power given to the LEAs to enable surveillance without prior judicial authorisation. It is possible that there was public awareness of the drafting of 2014 regulation given the effort to enable the LEAs to engage lawfully in

¹¹⁹⁰ Chapter 4, sec. 4.6.1.

¹¹⁹¹ Nigerian Communications Commission “Draft Lawful Interception of Communication Regulation” (2014) *Premium Times News* https://media.premiumtimesng.com/wpcontent/files/2014/05/LegalRegulations_Lawful_Interception_of_Communications-080113.pdf (accessed 2023-01-28).

communications surveillance, but there is certainly no record of public input in the LICR, the 2019 regulation which is now effective.

Another problem is that none of the laws provide information that defines the circumstances in which a person may become a subject of surveillance. Regulation 13 of the LICR provides merely that LEAs can apply for a communications surveillance order when they require information regarding a crime. Section 39 of the CPPA also focuses on the information to be intercepted. The TPPA does not specify whether information or the conduct of a person will result in the use of surveillance. It also provides the Attorney-General of the Federation, the Inspector-General of Police and the National Security Adviser with unfettered powers to execute communications surveillance as they deem fit in respect of terrorism-related offences. The focus of the laws is on the importance of the information to be obtained rather than the transparency of the process of surveillance and the protection of the right to privacy. The Nigerian legal framework therefore needs reform.

5.3.2.1 International law standard for accessibility of laws regulating communications surveillance

The international law requirement of accessibility of laws entails two stages: the pre-enactment and the enactment stages.¹¹⁹² The pre-enactment stage involves parliamentary debate, expert opinions and public input and criticisms. The enactment stage involves presidential assent in the case of statutes and the publication of the law to the public. All these processes, especially at the pre-enactment stage, provide transparency, accountability and public participation in the law-making process. The lack of pre-enactment accessibility may have contributed to the problem of overreach of the LICR, which is discussed in section 5.3.3 below.

The solution to this problem is also that a primary statute must be enacted. The pre-enactment stage will be very important to ensure that different perspectives on the proposed statute can be aired. Also, transparency at the pre-enactment stage will enable the public and especially legal experts to oppose any provision that may lead to arbitrariness or overreach.

¹¹⁹² 2014 OHCHR Report, par [29].

5.3.2.2 European regional law standard for accessibility of laws regulating communications surveillance

In *Zakharov v Russia*, the ECtHR held that laws regulating communications surveillance must be accessible to the public.¹¹⁹³ It also stated that even though technical documents detailing the actual surveillance techniques may not be available to the public, as they may jeopardise the surveillance effectiveness, these technical documents must not regulate communications surveillance.

These requirements are important for Nigeria to note. Technical documents must provide for strictly technical procedures, which can be a “classified document” and not made available to the general public. The proposed statute for Nigeria must identify the existence of these documents and provide specifically that parliament and the authorising body presiding on surveillance matters must have access to these technical documents in order to ensure accountability.

5.3.2.3 South African approach on accessibility of laws regulating communications surveillance

In South Africa, the laws that regulate communications surveillance, namely the RICA, Criminal Procedure Act (CPA)¹¹⁹⁴ and the Cybercrimes Act¹¹⁹⁵ are all accessible to the public. However, section 9 of the RICA, provides that regulations can be formulated and enacted for communications surveillance in prisons and then presented to parliament before publication in the Government Gazette.¹¹⁹⁶ This means that the regulations formulated under section 9 of the RICA do not undergo the pre-enactment stage and thus lack accessibility. Nigeria should avoid this loophole by ensuring that no parastatal is empowered to formulate laws (even subordinate ones) for communications surveillance. The LICR must therefore be repealed, as recommended below.

Even though the RICA meets the accessibility criteria in terms of its enactment procedure, some of its provisions were declared unconstitutional in *AmaBhungane*.¹¹⁹⁷ The main problem with the RICA is its inability to keep up with technological

¹¹⁹³ *Zakharov v Russia* pars [240-241]; Chapter 2, sec.5.2.

¹¹⁹⁴ Act 51 of 1977.

¹¹⁹⁵ Act 19 of 2020.

¹¹⁹⁶ This is discussed in section 5.3.1.3 of this chapter.

¹¹⁹⁷ *AmaBhungane v Minister of Justice* (CC) par [48, 94, 100, 108, 119, 135].

innovations that rendered communications surveillance more intrusive on privacy than was the case over two decades ago, when the RICA was enacted.¹¹⁹⁸ The statute regulating communications surveillance should therefore be reviewed from time to time in order to update it. This will enable the parliament to assess the impact of new technologies on the right to privacy and regulate its use accordingly.

5.3.2.4 Recommendations for Nigeria on accessibility of laws regulating communications surveillance

The problem of accessibility of the Nigerian legal framework on communications surveillance will be solved by ensuring that the proposed statute undergoes pre-enactment scrutiny. The scrutiny must not just be a formality, but a deliberate process involving experts in constitutional, human rights and international law in drafting the law. Also, public opinion must be sought through all media channels including social media platforms as this will enable more participation by those who are knowledgeable in ICT parlance and practice.

The documents describing technical procedures for surveillance must be accessible to the authorising body presiding on surveillance matters, and to parliament. In addition, these documents must not regulate the actual procedure for surveillance or the duty of CSPs. The statute must, however, specify that such technical documents exist to promote transparency. The technical documents must also be scrutinised by parliament to ensure that they do not provide any regulation for communications surveillance.

Furthermore, judicial input in the pre-enactment process of the proposed statute is important. Usually, judicial scrutiny occurs only once an enacted statute is challenged. Nevertheless, when there is an opportunity to scrutinise the statute in advance of its enactment, judges must not only declare provisions constitutionally invalid but also provide recommendations for its improvement.

¹¹⁹⁸ The ECtHR in *Bigbrother Watch v UK* App. nos. 58170/13, 62322/14, 24960/15 (2018) par [208] identified the issue of rapidly changing technology as the reason why it reversed its decision in *Weber and Saravia v Germany*, App. no. 54934/00, 2006-XI ECtHR 1173 where it declared that bulk surveillance does not infringe on article 8 of the ECHR.

5.3.3 Overreach of the laws regulating communications surveillance in Nigeria

The CPPA's overreach specifically concerns section 38 that enables LEAs to execute communications surveillance in respect of all crimes.¹¹⁹⁹ Also, the judicial guideline provided in the CPPA regarding the application for an interception order applies to cybercrimes only, even though the statute permits interception of communications for all crimes. This means that there is no criminal justice procedure for the interception of communications for crimes that are not cybercrimes.¹²⁰⁰

Regarding the LICR, its status as a subordinate law incapacitates it from regulating matters relating to law enforcement as this is within the purview of the legislature.¹²⁰¹ In addition, the legitimate aims for the interception of communications in the LICR are broader than those permitted for the limitation of the right to privacy in terms of section 45(1)(a) and (b) of the 1999 Nigerian Constitution.¹²⁰² The overbreadth is aggravated by the lack of proper definitions of the constitutional legitimate aims, as addressed in the previous section.

The aims for the interception of communication listed in Regulation 7(3) of the LICR are “interest of national security”,¹²⁰³ “preventing or investigating a crime”,¹²⁰⁴ “protecting and safeguarding the economic wellbeing”,¹²⁰⁵ “interest of public emergency or safety”¹²⁰⁶ and “giving effect to any international mutual agreements, which Nigeria is a party”.¹²⁰⁷ Most of these aims are not permissible limitations to the right to privacy under section 45(1) of the 1999 Nigerian Constitution.

The aims for permitting communications surveillance in the LICR that seem to align with section 45(1) of the 1999 Nigerian Constitution are the protection of the interest of national security and the investigation and prosecution of crimes.¹²⁰⁸ Chapter four highlighted how the terms “national security” and “defence” as utilised in section 45(1) differ.¹²⁰⁹ The chapter further demonstrated that the Nigerian courts have substituted

¹¹⁹⁹ S.39 of the CPPA.

¹²⁰⁰ Interception of communication as defined in chapter one refers to an interception of the content of electronic communications.

¹²⁰¹ Schedule 1, Exclusive Legislative List 1999 Constitution.

¹²⁰² Chapter 4, sec. 4.8.3.4.6.

¹²⁰³ Regulation 7(3)(a) of the LICR.

¹²⁰⁴ Regulation 7(3)(b) of the LICR.

¹²⁰⁵ Regulation 7(3)(c) of the LICR.

¹²⁰⁶ Regulation 7(3)(d) of the LICR.

¹²⁰⁷ Regulation 7(3)(e) of the LICR.

¹²⁰⁸ Regulation 7(3)(b) of the LICR.

¹²⁰⁹ Chapter 4, sec. 4.6.3.

defence for national security.¹²¹⁰ This is why it is argued above that the “interest of national security” utilised in the LICR aligns with section 45(1). Nonetheless, the “interest of national security” is broadly stated because it is not defined in the context of surveillance.

The protection of the rights and freedom of others, an aim for limitation in section 45(1), could potentially encompass “for the purpose of investigating or preventing a crime” which is listed in the LICR as an aim for communications surveillance. However, the nature of the offences that can result in communications surveillance are not specified. Instead, there is a broad provision permitting surveillance for the prevention and investigation of crimes. While criminal justice procedures are a permissible limitation for the right to privacy, they must be narrowly defined to include serious crimes only to ensure that the right to privacy is protected during the execution of surveillance.

Chapter four further defined other legitimate aims in section 45(1).¹²¹¹ These other aims are public morals, public health, public order and public safety. No other aim in Regulation 7(3) of the LICR, save for the “interest of public safety”, fits into any of the definitions of these legitimate aims. The LICR therefore includes aims that are not compatible with the permissible limitation to the right to privacy in section 45(1) of the 1999 Nigerian Constitution. It is clear that reform is necessary.

5.3.3.1 International law standard on overreach of the laws regulating communications surveillance

The 2014 report of the OHCHR on the right to digital privacy states that “lawfulness” of communications surveillance should be tested against the Member State’s Constitution and international law.¹²¹² Any legislation on communications surveillance is unlawful if it does not align with the Constitution and/or international law. The overreach of the LICR in terms of the limitation of rights in the 1999 Nigerian Constitution renders it unlawful and not aligned with international law standard.

The proposed new statute must provide for constitutionally recognised aims for executing communications surveillance. The permissible aims for employing communications surveillance are the protection of national security, preservation of

¹²¹⁰ Chapter 4, page 199.

¹²¹¹ *Ibid.* The legitimate aims in section 45(1) are defined in a manner that aligns with international law using the Siracusa Principles Document.

¹²¹² 2014 OHCHR Report, par [28].

public order and public safety, public health, public morals and for the protection of the rights and freedom of others. These, however, must be narrowly defined in order to avoid overreach. The law would also have to be a justifiable limitation to the right to privacy discussed in section 5.2.2 above.

5.3.3.2 Regional and foreign law standard on overreach of laws regulating communications surveillance

This sub-section discusses both African and European law together with the South African law as the observations gathered from these legal systems are short and ultimately underpinned by international law. The European jurisprudence has not yet specifically addressed the issue of overbreadth of laws. The South African Constitution does not provide specific legitimate aims for limiting rights, unlike the 1999 Nigerian Constitution. The AU law in Article 41(2) of the 2019 Declaration provides that communications surveillance must be utilised for serious crimes and other legitimate aims. The 2019 Declaration does not, however, specify the legitimate aims other than serious crimes for executing communications surveillance.

Had there been a right to privacy in the ACHP, there would have been legitimate aims for its limitation which could then be applied to communications surveillance. Consequently, Member States have the discretion to determine the appropriate legitimate aims for communications surveillance. These aims must conform with international human rights law. International law is therefore the only reference for Nigeria with regard to the problem of this aspect of the overbreadth in the LICR.

5.3.4 Lack of safeguards for the acquisition of the metadata of communications

In chapter one metadata was defined as information automatically generated during electronic communications.¹²¹³ It includes information on the time of the communication, the parties to the communication, the devices used to communicate, and the location of the communication.”¹²¹⁴ The TPPA and the LICR have no explicit provisions regarding the acquisition of metadata. **Yet, very strangely, the LICR actually**

¹²¹³ Chapter 1, sec.1.1; Geist “Why Watching the Watchers Isn’t Enough: Canadian Surveillance Law in the Post-Snowden Era” *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (2015) University of Ottawa Press 229; 2014 OHCHR Report, par [20]; National Information Standards Organization “Understanding Metadata” (2004) NISO Press, www.niso.org/publications/press/UnderstandingMetadata.pdf (accessed 2021-01-10).

¹²¹⁴ *Ibid.*

defines metadata (which it refers to as communications data) as any traffic data, that is attached to an electronic communication or, not being the content of the communications, involves the use of a communications service or network.¹²¹⁵ Although, the CPPA enables the lawful acquisition of metadata, it does not provide for judicial authorisation for the acquisition of metadata.¹²¹⁶ As a result, LEAs are permitted to request a CSP to provide metadata and the latter will be compelled to comply.¹²¹⁷

The only precaution for the use of metadata in the CPPA is that “due regard” must be given to the right to privacy of the subject of surveillance while acquiring metadata.¹²¹⁸ Unfortunately, there are no provisions enumerating how this “due regard” is to be provided or tested. This is another example of an abstract provision that provides no concrete protection for the right to privacy. While the CPPA provides that metadata must be utilised for legitimate purposes and kept confidential,¹²¹⁹ there is no specific provision on the procedure for ensuring the confidentiality of the metadata obtained.

5.3.4.1 International law standard on the acquisition of metadata

In chapter two it was shown that the intrusive nature of metadata has evolved over the years.¹²²⁰ Innovations with the technology used to acquire metadata has developed so rapidly that it is now as intrusive as the interception of content of communication.¹²²¹ That is, metadata can now provide information that is as accurate as the content of communications. Hence, the same level of protection should be afforded to both.¹²²² This means that domestic laws on communications surveillance that do not provide adequate protection for rights while permitting the acquisition of metadata will be unlawful and arbitrary.¹²²³

¹²¹⁵ Regulation 23 of the LICR.

¹²¹⁶ Chapter 4, sec. 4.8.1; S.38(1) of the CPPA.

¹²¹⁷ S.38(2) of the CPPA.

¹²¹⁸ S.38(5) of the CPPA.

¹²¹⁹ S.38(4) and (5) of the CPPA.

¹²²⁰ Executive Office of the President, “Big Data and Privacy: A Technological Perspective” (1 May 2014) <https://obamawhitehouse.archives.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy> (accessed 2021-06-10) 19.

¹²²¹ 2014 OHCHR Report, par [19].

¹²²² Court of Justice of the European Union, Judgment in joined cases C-293/12 and C-594/12; *Digital Rights Ireland v Minister for Communications, Digital Rights Ireland and Seitlinger*, Judgment of 8 April 2014, pars [26-27, 37].

¹²²³ 2014 OHCHR Report, par [20].

The Nigerian legal framework on communications surveillance fails to provide adequate protection for rights while permitting the use of metadata and is therefore unlawful and arbitrary. The solution is for the proposed law to provide the same protection of the right to privacy when permitting interception of communications and acquisition of metadata. This means that the proposed statute must provide that LEAs must apply to a judge for the acquisition of metadata, using the same procedures as for the content of communications. It should be noted that the emphasis must be on adequate safeguards to the right to privacy and the difference in technical approaches should not negatively affect the protection of the right to privacy. The difference between these two types of communications should be reflected in the proposed statute, albeit for ease of reference, and not for affording lesser protection.

5.3.4.2 European regional jurisprudence on the acquisition of metadata

The Court of Justice of the European Union (CJEU) has more specific jurisprudence on metadata. This is because in *Schrems v Facebook Ireland Ltd*, the CJEU declared that articles 1(2) and 5(2) of Directive 2006/24/EC on the retention of data infringes article 8 of the Charter of Fundamental Rights of the European Union (EU Charter) by providing lesser protection for metadata.¹²²⁴ The CJEU also acknowledged the ECtHR's minimum requirement and applied it to issues relating to surveillance and stated that the same interpretation must be given to the privacy rights in the EU Charter and ECHR.¹²²⁵ Hence, the European jurisprudence on metadata is that its acquisition must align with the ECtHR's minimum requirement. This also means that the same protection afforded to a person while intercepting the content of their communication, must be extended to the metadata of the communication. The position on metadata in the European jurisdiction also aligns with international law. Nigeria's proposed statute must provide similar procedures that adequately protects the right to privacy for both

¹²²⁴ *Schrems v Facebook Ireland Ltd* App. No C-498/16 (2018) par [94]; *Digital Rights Ireland v Minister for Communications, Ireland Digital Rights Ireland and Seitlinger*, C-293/12 and C-594/12, EU:C:2014:238, Judgment of 8 April 2014, par [39].

¹²²⁵ *Nowak v Data Protection Commissioner*, App. No. C-434/16 (2017); *Schrems v Facebook Ireland Ltd* App. No C-498/16 (2018); *Google Spain v Google* C-131/12 (2014); *GC v CNIL* App. No. C-136/17(2019); *Digital Rights Ireland*; *Secretary of Home Department v Watson* App. No. C-201/15 and C-698/15 (2018); *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* EU Official Journal, App. No. C22 22/1/18 29-30 (2017).

the content of communication and metadata. The full recommendation regarding this problem is highlighted in 5.3.4.4 below.

It is recommended that the proposed new statute should have a single procedural guideline for both acquisition of metadata and the interception of content of communications. This means that, unlike the current legal framework on communications surveillance in Nigeria, LEOs will now be required to apply for judicial authorisation to acquire metadata. LEOs will then need to apply for the acquisition of metadata only when it serves a legitimate purpose.

5.3.4.3 South African approach on the acquisition of metadata

The RICA classifies electronic communications into three categories namely, the content of communication, real-time communication-related information and archived information-related communication. The RICA refers to metadata as information-related communication. This classification is supposedly to differentiate the kinds of information involved in communications surveillance. However, the only difference between real-time and archived communication-related information is that the former relates to metadata acquired within 90 days of the communication and the latter to metadata obtained after 90 days of the communication. The differentiation of the kinds of communications creates a hierarchy of protection with the content of communication ranking highest, followed by real-time communication-related information. This kind of definition should be avoided in the proposed statute for Nigeria as the intrusiveness of metadata on the right to privacy does not diminish with the duration of its acquisition.

The division of metadata into real-time and archived communication-related information diminishes the quality of safeguards afforded to the right to privacy during the acquisition of archived communication-related information. Meanwhile, the definition of the term “real-time” in the RICA is different from its common usage where it refers to the actual time when an event occurs. This definition is misleading. This may be the reason why Justice Sutherland, while adjudicating the *AmaBhungane* case in the High Court confused interception of the content of communication with real-time surveillance.¹²²⁶ The proposed statute for Nigeria should avoid providing a different

¹²²⁶ *AmaBhungane v Minister of Justice* 2020 (1) SA 90 (GP) par [33]. RICA does not differentiate between surveillance conducted in “real time” and that conducted thereafter. The differentiation of whether communication is “real time” or not does not have any noticeable effect on its intrusion on privacy. While it may be relevant for technical accuracy, it has no impact on the overall protection of the right to privacy.

meaning for terms that already have a known definition in ICT parlance as this will cause confusion. Hence real-time surveillance will be defined as surveillance of any type of electronic communications in which all users can exchange information instantly or with negligible latency or transmission delays.”¹²²⁷ In other words, communications surveillance of “live” information exchange over an electronic communications network is referred to as “real-time surveillance.”

While the division of content of communication and metadata was consistent with the technological innovation at the time of the enactment of the RICA, there is no visible technical difference between archived and real-time communication-related information.¹²²⁸ The division of metadata into real-time and archived communication-related information therefore serves no purpose in relation to the protection of the right to privacy. The proposed statute for Nigeria should avoid providing a different classification of metadata. Hence, the Nigerian provisions should state that guidelines are for communications surveillance, rather than providing different guidelines for metadata and content of communications.

South Africa’s approach to the surveillance of metadata is useful only to the extent that it has a detailed classification system and good procedural guidelines for each kind of communication. Classification of communications is beneficial when it is used to clarify the difference between metadata and content of communications and this can be done in the definition section. It is recommended that the definition section in the proposed Nigerian law should stipulate the difference between the two aspects of communications surveillance by defining metadata and content of communications. Afterwards, the provisions in the proposed new statute should relate to communications surveillance as a whole concept.

5.3.4.4 Recommendation for Nigeria on the acquisition of metadata

The proposed Nigerian statute for communications surveillance in Nigeria must contain provisions that recognise metadata. This term must be defined, preferably in line with its popular usage. The definition of metadata provided in chapter one should be adopted in Nigeria in order to avoid any confusion. Also, metadata must be

¹²²⁷ Irei “Guide to Building an Enterprise Unified Communications Strategy” <https://searchunifiedcommunications.techtarget.com/definition/real-time-communications> (accessed 2021-10-24).

¹²²⁸ *AmaBhungane v Minister of Justice* par [28].

afforded the same level of protection as the content of communication.¹²²⁹ This protection will include LEAs applying to a judge for a communications surveillance order to acquire metadata. The procedural guidelines for the application must be similar to the application used to acquire the content of the communication and provide adequate safeguards for the right to privacy. Recommendations for effective procedural guidelines for Nigeria are discussed in section 5.4 below.

In addition, metadata and the content of an electronic communication should not be classified separately in the proposed new statute. The sections should use headings such as “procedural guidelines for communications surveillance” and “pre-authorisation procedure for communications surveillance”. This will ensure that the same procedural guidelines for content of communications applies to the acquisition of metadata as well. The difference in the technical requirements should be contained in the technical documents that details the actual techniques of executing communications surveillance and not in the statute.

5.4 The development and implementation of sound and fair procedural rules at all stages of communications surveillance

Communications surveillance consists of three stages. They are the pre-surveillance (authorisation procedure), the execution (or implementation) stage and the post-surveillance stage.¹²³⁰ The pre-surveillance stage includes the application for a communications surveillance order from a judge while the execution stage involves the implementation of the surveillance order. The post-surveillance stage relates to the processing and preservation of information obtained from the surveillance. All these stages are poorly regulated by the Nigerian laws on communications surveillance, which enable its arbitrary use. The next sub-sections discuss the problems with the procedural rules of the regulation of communications surveillance in the Nigerian laws regulating communications surveillance. They also recommend the development of new procedural rules by applying the lessons drawn from international,

¹²²⁹ The Court of Justice of the European Union also recommends that the same safeguard that is afforded to the right to privacy during communications surveillance also applies to the acquisition of metadata. *Digital Rights Ireland* par [54]; *Liberty v United Kingdom*, App. No.58243/001, (2008) par [62-63]; *Rotaru v. Romania*, App. No.28341/95, (2000) pars [57-59]; *S. and Marper v United Kingdom*, App. Nos.30562/04 and 30566/04, (2008) par [99]; *M.K. v France*, App. No.19522/09, (2013), par [35].

¹²³⁰ *Klass v Germany*, App. No. 5029/71 (1978) par [55]; *Zakharov v Russia* par [233].

African and European regional law and the South African framework to recommend reform for the current communications surveillance regime in Nigeria.

5.4.1 Problems with the pre-surveillance stage

The problem with the pre-surveillance stage is that the current legal framework is ineffective and provides little safeguard for the right to privacy. The procedural guidelines in the CPPA and the LICR are vague. The laws also encourage the impunity of the LEO, as they do not provide a means for verifying the truth of the information supporting the surveillance applications.

In addition, no provision is made in the TPPA and the LICR for sanctioning LEOs who apply for a communications surveillance order based on false evidence. This is because neither of the laws require supporting information for the surveillance application to be on oath, hence LEOs applying for surveillance orders based on false pretences cannot be charged with perjury. The laws therefore do not prevent the falsification of information that supports a communications surveillance application. These laws lack safeguards against abuse of communications surveillance. These problems are now discussed in detail.

5.4.1.1 The provision of the TPPA on the pre-surveillance stage

The TPPA provides for an internal reporting mechanism prior to the application for a surveillance order. This internal reporting mechanism requires the National Security Adviser (NSA) to approve the applications for communications surveillance before it is filed in court.¹²³¹ The internal safeguards are prone to abuse without a corresponding independent oversight mechanism.¹²³² In addition, the internal guidelines do not affect the protection of the surveillance subject's rights to privacy. The decision to authorise surveillance is solely within the judge's discretion.¹²³³

Another problem is that the TPPA provides that a judge should authorise a communications surveillance order but does not include procedural guidelines for the judicial authorisation.¹²³⁴ This gives judges unrestrained discretionary power in

¹²³¹ S.29 of the TPPA.

¹²³² General Assembly, Resolution 68/167, 68th session, Agenda 69(b), "The Right to Privacy in the Digital Age" on 18 December 2013, 2.

¹²³³ S.29 of the TPPA.

¹²³⁴ *Ibid.*

authorising surveillance orders. This procedure therefore lacks transparency and it is prone to abuse.

5.4.1.2 The provision of the CPPA on the pre-surveillance stage

The CPPA has abstract procedural guidelines. It provides that a judge can authorise communications surveillance if there are reasonable grounds to believe that a person or material, for example a computer, on a property is relevant to the investigation of a cybercrime.¹²³⁵ The court will then authorise the surveillance when it is satisfied that it is necessary to prevent a cybercrime or to prevent an interference with an investigation relating to a cybercrime.¹²³⁶ The term “reasonable ground”, without any supporting definition of what it entails, is vague and relies solely on judges’ subjective opinions. This gives the judges wide discretionary powers and also creates vague laws, as the expected standard is not specified

In addition, the factors determining the authorisation of communications surveillance are based on whether the applicant can convince the judge that a cybercrime has been committed or is about to be committed, and that the surveillance subject will provide some information. Authorisation is not based on evidence establishing the surveillance subject’s involvement in the crime. In other words, the applicant need only to prove some kind of relevance between the surveillance subject and the cybercrime, not an involvement of the subject in the crime.

This situation is exacerbated by the high possibility of limited information being presented to the judge, as there is no provision that the judge must be presented with all the relevant information. LEAs could omit information that does not favour their application in order to ensure a successful outcome. Although the CPPA requires the supporting information to be submitted under oath, there is no practical means of verifying the truth of the information.¹²³⁷ As a result, communications surveillance under the CPPA has a high probability of being authorised based on false or misleading evidence.

This approach does not adequately safeguard the right to privacy, because a communications surveillance order is unlike other warrants. In their case, the

¹²³⁵ S.45(2)(d) of the CPPA.

¹²³⁶ S.45(1) and 2(a)-(c) of the CPPA.

¹²³⁷ S.45(1) of the CPPA.

defendants become aware of the warrants during their execution and can challenge any unlawful action or the judge's decision. In the case of communications surveillance, however, the success of the procedure depends on the surveillance subject's ignorance. Redress is only available, if at all, once the whole process of the surveillance is complete. It is therefore very important that the authorisation stage of communications surveillance leave little room for arbitrariness, which is not the case with the CPPA. Reform is, therefore, needed.

5.4.1.3 The provisions of the LICR on the pre-surveillance stage

The LICR's procedural guideline is problematic because, just like the CPPA, its basis for the granting of a communications surveillance order is vague. Regulation 13(3)(a) of the LICR provides that the supporting facts must be "reasonable and persuasive enough to believe that any of the matter mentioned in regulation 7(3) of these Regulations [aims for surveillance] has occurred, is occurring or about to occur".¹²³⁸ It does not specify for which facts provision has to be made for the granting of a surveillance order to be considered "reasonable and persuasive" enough to believe that there is a legitimate aim for executing communications surveillance.¹²³⁹ Again, the judge has a wide discretion to determine what is considered "reasonable and persuasive enough" to believe that one of the legitimate aims for authorising a surveillance order has occurred.¹²⁴⁰

In addition, most of the information supporting the application does not have to be given under oath.¹²⁴¹ Hence, in terms of the LICR, there are no repercussions for an applicant providing false evidence. This is particularly ineffective for safeguarding the right to privacy because the issue of LEAs falsifying evidence to procure a communications surveillance order is a global phenomenon.¹²⁴² It is clear that, legislators enacting laws regulating surveillance must take care to ensure that the truth of information supporting the surveillance application can be verified.

¹²³⁸ Regulation 13(3)(a) of the LICR.

¹²³⁹ *Ibid.*

¹²⁴⁰ *Ibid.*

¹²⁴¹ Regulation 12(3)(e) of the LICR.

¹²⁴² *AmaBhungane Centre for Investigative Journalism v Minister of Justice* 2021 (4) BCLR 349 (CC) par [40]; *Klass v Germany* par [59]; The head of argument of the Plaintiffs in *AmaBhungane v Minister of Justice* https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf (accessed on 2020-02-10).

Furthermore, the LICR provides that the judge must have full access to all relevant information relating to the application.¹²⁴³ It must also pertain to the permitted aims for surveillance under Regulation 7(3) and be supported by information obtained under oath stating that there are no other means to obtain the information.¹²⁴⁴ These provisions, even though providing more safeguards than the CPPA and the TPPA, have little positive impact on the right to privacy because the LICR is lower in hierarchy than the CPPA and the TPPA.

Another problem with the LICR's procedural guidelines is that Regulation 12(4), which permits LEAs in certain circumstances to delay prior judicial authorisation for 48 hours, leaves room for arbitrary application. Regulation 12(4) provides that:

“Notwithstanding the provisions in this Regulations, an Authorised Agency may initiate interception of Communications without a warrant in the event of-

- (a) immediate danger of death or serious injury to any person;
- (b) activities that threaten the national security;
- (c) activities having characteristics of organised crime;

provided that the Authorised Agency shall apply for a Warrant to the Judge within 48 hours after the interception has occurred or began to occur before issuance of a Warrant for such interception and where the application is not made, or denied within 48 hours, the interception shall terminate immediately and further interception shall be treated as unlawful.”

There are three problems with this provision. First, only the activity in Regulation 12(4)(a) is of an urgent nature, whilst the others do not always regulate urgent matters. This seems to be a provision that is tailored to aid LEAs to execute communications surveillance without prior authorisation. Secondly, the activities mentioned in Regulation 12(4)(b) and (c) are not defined. As a result, LEAs can execute communications surveillance if in their perception the activity falls under these exceptions, even if it does not. It thus leaves LEAs with an unlimited degree of discretion which increases the possibility of abuse.

Thirdly, LEAs may apply to the judge within 48 hours of the surveillance executed in terms of Regulation 12(4) if they are unable to complete the interception within that time. This means that had the interception been completed within 48 hours, judicial authorisation would be unnecessary. Practically, there is no reason to apply for judicial authorisation if LEAs can simply execute communications surveillance and ensure its completion within 48 hours. More so, they can just copy all the surveillance subject's

¹²⁴³ Regulation 12(3)(a) and (b) of the LICR.

¹²⁴⁴ Regulation 12(3)(c) of the LICR; Regulation 12(3)(e) of the LICR.

communications from the CSPs and peruse it at their convenience. Even when the judge is notified of the surveillance, there is no provision to review the lawfulness of the surveillance that has already been executed prior to the application. Thus, information gathered from an unlawful surveillance within the 48-hour window is not destroyed. This constitutes an unjustifiable infringement on the surveillance subject's right to privacy.

Ultimately, the pre-surveillance procedure in the Nigerian legal framework accommodates abuse and arbitrariness because of the poor procedural guidelines for the authorisation process. There is a need for specific and clear guidelines that can effectively safeguard the right to privacy during the authorisation process. Procedural rules assist the judge in ascertaining the factors that must be considered before an order is granted. This ensures that the judge is guided in ensuring that the right to privacy of the surveillance subject is adequately protected. Also, a guideline that can ensure the transparency of the process and objectivity of the judges in authorising a communications surveillance order is necessary.

International law provides a broad guideline for the protection of the right to privacy and specifically with regard to the utilisation of communications surveillance. European regional law provides practical provisions for a law regulating communications surveillance. These can be contextualised and adopted into the proposed statute for Nigeria. South African law also provides good examples for Nigeria to emulate and some loopholes to avoid. These laws are discussed in the next sub-sections.

5.4.1.4 International law standard on the pre-surveillance stage

The international law standard for domestic laws regulating communications surveillance requires that “[A]ny restriction may not be unduly vague or overbroad such that it could confer unfettered discretion on officials”.¹²⁴⁵ This means that procedural guidelines for the application of a communications surveillance order must be clear, precise, comprehensive and ensure transparency of the surveillance process.

Lawfulness in terms of the ICCPR requires States to refrain from “secret rules and secret interpretations – even secret judicial interpretations – of laws”.¹²⁴⁶ This provision

¹²⁴⁵ Special Rapporteur's Report on the promotion and protection of the right to freedom of opinion and expression “surveillance and human rights” A/HRC/ 41/35 (2009) par [24].

¹²⁴⁶ 2014 Report of the OHCHR par [29].

means that all interpretation of laws regarding communications surveillance by the judiciary must be publicly available to enable individuals to be well-informed about the law with sufficient precision.¹²⁴⁷ Laws must also not provide unrestrained executive authority or excessive discretionary powers.¹²⁴⁸ International law further requires Member States to provide “effective procedural safeguards, including effective, adequately resourced institutional arrangements” when utilising communications surveillance.¹²⁴⁹ This enables a surveillance subject to have “protection of the law” as provided by article 17 of the ICCPR.¹²⁵⁰

A weak procedural safeguard for communications surveillance equates an absence of the protection of the law and leaves surveillance subjects vulnerable to unlawful and arbitrary interference with their right to privacy.¹²⁵¹ International law also requires an independent and external oversight mechanism to monitor all stages of communications surveillance. These may include an independent civilian oversight.¹²⁵²

Finally, Resolution No. 68/167 on the Right to Privacy in the Digital Age calls upon Member States:

- “(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;
- (d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;”¹²⁵³

International law is clear that an effective procedural guideline is one of the elements of a communications surveillance regime that is lawful and non-arbitrary. However, these guidelines are broad and they do not stipulate specific minimum requirements

¹²⁴⁷ Human Rights Committee “Concluding Observations of the Fourth Period Report of the United States of America” CCPR/C/USA/CO/4, 23 April 2014, par [22]. The Human Rights Committee raised concerns regarding the decisions of the United States Foreign Intelligence Surveillance Court (FISC) that had “largely been kept secret”.

¹²⁴⁸ *Ibid.*

¹²⁴⁹ 2014 Report of the OHCHR par [37].

¹²⁵⁰ *Ibid.*

¹²⁵¹ *Ibid.*

¹²⁵² *Ibid.*

¹²⁵³ General Assembly, Resolution 68/167, 68th session, Agenda 69(b), “The Right to Privacy in the Digital Age” on 18 December 2013, 2.

with concrete provisions that can be adopted into a proposed statute for Nigeria. This may be because the Human Rights Committee have not presided over cases that deals specifically with communications surveillance. Nigeria should be mindful of the broad guidelines in international law while drafting its proposed statute. However, European regional law is more useful in providing practical requirements that will safeguard the right to privacy at all stages of communications surveillance in the proposed statute.

The next sub-section discusses African regional law's standard regarding procedural guidelines for communications surveillance. However, the African regional law like international law provides a broad guideline only. It is briefly mentioned in 5.4.1.5 below. European regional law is more useful in providing practical requirements that will safeguard the right to privacy at all stages of communications surveillance in the proposed statute. It is therefore discussed in more detail in the subsequent sub-sections and contextualised to form the basis of the provisions in the proposed new statute for Nigeria.

5.4.1.5 African regional law standard on the pre-surveillance stage

Principle 41(3) of the 2019 Declaration provides that a law on communications surveillance which has adequate safeguards for the right to privacy must include the following:

- a. the prior authorisation of an independent and impartial judicial authority;
- b. due process safeguards;
- c. specific limitation on the time, manner, place and scope of the surveillance;
- d. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
- e. proactive transparency on the nature and scope of its use;"

Principles 41(3)(a), (c) and (d) are broad guidelines that can be interpreted and contextualised by Member States in a way that does not provide adequate protection to the right to privacy.

It would have been helpful if the 2019 Declaration had elaborated on the meaning of "due process safeguard" by providing specific procedures that should be followed, for example, provisions requiring that laws must be sufficiently clear and foreseeable. Also, Principle 41(3)(d) could further state what qualifies as a "reasonable time" for post-surveillance notification. Lastly, Principle 41(3)(e) could specify the nature and

scope of the use of communications surveillance by providing a list of legitimate aims that may prompt surveillance.

The absence of specific guidelines creates difficulty in adopting these Principles into domestic laws. It also jeopardises uniformity among laws regulating communications surveillance of Member States of the AU. Thus, like international law, African regional law does not provide practical procedural guidelines on communications surveillance that Nigeria can adopt directly into its new statute. The European regional law is far more detailed. The following subsections therefore focus on utilising the specific guidelines in European regional law to address the problems associated with the procedural guidelines in the Nigerian laws on communications surveillance.

5.4.1.6 European regional law standard on the pre-surveillance stage

In the European region, the ECtHR has held that laws regulating surveillance must provide sufficient clarity regarding the manner in which the persons charged with oversight duties exercise the discretion that is conferred on them.¹²⁵⁴ The Court has also held that the authorisation procedure must be “capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration”.¹²⁵⁵ The ECtHR in *Zakharov v Russia* scrutinised the Russian’s procedural guideline on communications surveillance and it recommended solutions to the problems that were identified within the Russian legal framework.¹²⁵⁶ These are similar to the flaws in the Nigerian legal framework. The judgement in *Zakharov v Russia* is therefore useful.

In *Zakharov v Russia*,¹²⁵⁷ the ECtHR stated that the established judicial interpretation of terms can assist in explaining vague provisions in surveillance law. The Court also declared that there must be an established practice or judicial precedent on which the exercise of a judicial discretion is based.¹²⁵⁸ This ensures that there is a practice that ensures that sufficient reasons exist for communications surveillance in each case.¹²⁵⁹ The ECtHR further declared that the “possibility of improper action by a dishonest, negligent or overzealous official can never be completely ruled out whatever the

¹²⁵⁴ *Zakharov v Russia* par [247]; *Liu v Russia*, No. 42086/05, 6 December 2007 par [56].

¹²⁵⁵ *Zakharov v Russia* par [257].

¹²⁵⁶ *Zakharov v Russia* par [261].

¹²⁵⁷ *Zakharov v Russia* par [249].

¹²⁵⁸ *Ibid.*

¹²⁵⁹ *Ibid.*

system”.¹²⁶⁰ The surveillance regime must thus not be set up in such a way that it is prone to abuse.

The ECtHR held that grounds for authorisation of a communications surveillance order must not be vague.¹²⁶¹ Grounds, such as “reasonable suspicion” as the basis for secret surveillance, must be accompanied by specific definitions.¹²⁶² Also, the law must specify that applicants must provide specific reasons, backed by evidence, of why they suspect a person’s involvement in any activity can legitimately make them surveillance subjects.¹²⁶³ This enables judges to determine whether there is a sufficient factual basis to authorise a communications surveillance order.¹²⁶⁴

Specific definitions of terms set out in the law regulating communications surveillance is an important lesson for Nigeria. As discussed in section 5.2.2 above, there is a dearth of judicial precedent on the definition of legitimate aims in section 45(1)(a) and (b) of the 1999 Nigerian Constitution. Hence, the proposed Nigerian statute cannot depend on Nigerian judicial precedent to provide definitions of vague provisions and the statute must provide its own clear and specific provisions that are neither vague nor ambiguous. The ECtHR also held that laws on communications surveillance must specify that judges must be provided with all relevant facts that will enable them to conduct a proportionality and necessity test.¹²⁶⁵ It is also important that the authorising body has full access to all relevant facts as this will enable it to determine whether there is a reasonable suspicion that one of the legitimate aims for communications surveillance exists.¹²⁶⁶

Relying on grounds for applying for a surveillance order such as “reasonable suspicion”, “reasonable ground” and “reasonable and persuasive enough” is not problematic if the grounds are defined. However, the absence of full access to information by the authorising body that will assist in determining the existence of the grounds also causes vagueness. The proposed statute must, therefore empower the

¹²⁶⁰ *Zakharov v Russia* par [270].

¹²⁶¹ *Zakharov v Russia* par [259].

¹²⁶² *Zakharov v Russia* pars [261-263]; *Liu v Russia* pars [59-63]; *Chahal v United Kingdom*, 15 November 1996, App. no. 22414/93, par [131].

¹²⁶³ *Zakharov v Russia* par [260].

¹²⁶⁴ *Zakharov v Russia* par [261].

¹²⁶⁵ *Zakharov v Russia* par [192]. In addition, the use of “reasonable suspicion” reflects the African regional law standard on the ground for evaluating application for communications surveillance orders. This is discussed in 5.3.1.2 above.

¹²⁶⁶ *Zakharov v Russia* par [192].

authorising authority on surveillance matters to obtain full access to all relevant information relating to the surveillance application.

Full access to all information also includes an avenue for verifying the truth of the information provided.¹²⁶⁷ In addition, it includes the application identifying a specific person by stating “their names, telephone numbers to be tapped, address and other relevant information”.¹²⁶⁸ This will reduce the tendering of false evidence and also enables judges to verify that the aims for executing communications surveillance are legitimate and whether they can be achieved by less intrusive means.¹²⁶⁹ Access to full information relating to the surveillance application broadens the scope of judicial scrutiny and enables a detailed inquiry into the facts provided by the LEO.¹²⁷⁰ The proposed Nigerian statute must therefore provide full access to the authorising body to enable it to scrutinise surveillance applications effectively, which must be stated in very clear terms.

Finally, on the appropriate procedure for waiver of prior judicial authorisation, the ECtHR recognises that there will be situations that will require urgency and for which it will not be expedient to request authorisation.¹²⁷¹ However, the ECtHR has stated that the law must specify that the waiver of prior authorisation must be permitted in urgent situations only and it must be “used sparingly and only in justified cases.”¹²⁷² Otherwise, authorities will be left with an unlimited discretion to decide when to use the urgency procedure and this will lead to abuse.¹²⁷³ If the waiver provision is inadequately framed, it will provide LEAs with an avenue to circumvent judicial authorisation.¹²⁷⁴ Judicial supervision is one of the most important safeguards for the right to privacy during surveillance and its waiver must be temporary.¹²⁷⁵ Also, the

¹²⁶⁷ *Zakharov v Russia* par [260]; *Klass v Germany* par [51]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, Application no.62540/00, 28 June 2007, par [79-80]; *Iordachi v Moldova* par [51]; *Kennedy v United Kingdom*, pars [31-32].

¹²⁶⁸ *Zakharov v Russia* par [264]; *Liberty v United Kingdom* pars [64-65]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, par [80]; *Dimitru Popescu v Romania* (no.2), Application no. 71525/01, 26 April 2007, par [78]; *Kennedy v United Kingdom*, par [160].

¹²⁶⁹ *Liu v Russia* pars [59-63]; *Chachal v United Kingdom*, Report 1996-V par [131]; *Zakharov v Russia* par [261].

¹²⁷⁰ *Zakharov v Russia* par [261].

¹²⁷¹ *Zakharov v Russia* par [266].

¹²⁷² *Ibid.*

¹²⁷³ *Ibid.*

¹²⁷⁴ *Ibid.*; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* pars [16 and 82].

¹²⁷⁵ *Zakharov v Russia* par [266].

surveillance conducted without authorisation must be subject to the review of the oversight mechanism.¹²⁷⁶

Regulation 12(4)(a) of the LICR provides for a waiver of preauthorisation of communications surveillance where there is imminent danger. This is the only provision in the LICR that indicates an urgency of the situation and requires a waiver of preauthorisation of communications surveillance. Other activities mentioned in Regulation 12(4)(b) and (c) of the LICR have no urgency attached to them and the preauthorisation waiver afforded the activities is unjustifiable.

The proposed statute must therefore state that waiver of judicial authorisation must only take place in urgent situations or in emergencies (which must be defined). There must also be judicial notification of such execution within 24 hours of its commencement and the execution of surveillance prior to the authorisation must be submitted to the judge for review. If the application for authorisation is denied, the details of the surveillance activities that have been executed must be submitted and must be discontinued and destroyed immediately.

5.4.1.7 South African approach on the pre-surveillance stage

Sections 16 to 19 of the RICA provide procedural guidelines for communications surveillance. These procedural guidelines are divided into three sections and are prescribed in the order of hierarchy that the RICA accords to different types of communications surveillance. Section 5.4.2 above demonstrated that less protection is available for the right to privacy during the acquisition of metadata compared to the content of communication. The result is that the interception of the content of communication is at the top of the hierarchy, followed by real-time communication-related information, and finally archived communication-related information at the bottom end.

The procedural guideline for the interception of the content of communications in the RICA provides the best protection for the right to privacy in the South African legal framework. Thus, it will be used in this section to proffer solutions for the problems in the Nigerian laws on communications surveillance relating to its procedural guidelines. This is not saying that this South Africa's procedure for the interception of content of

¹²⁷⁶ *Zakharov v Russia* par [266].

communications is perfect, but it does contain some good examples for Nigeria, together with some loopholes that must be avoided. Furthermore, the Constitutional Court held that "... legislation infringing on the right to privacy is required to limit the officials' discretion as much as possible."¹²⁷⁷ Hence, legislation on communications surveillance must provide detailed guidance to LEAs that will minimise wide discretionary powers.

Section 16 of the RICA provides the procedural guideline for the interception of the content of communication. Section 16(1) sets out for the information that must be included in the application for an interception order. This information includes that the applicant must provide the name of the surveillance subject and the law enforcement agent that will execute the order, if known.¹²⁷⁸ Although the name of the surveillance subject is optional in the application, the situation is different in practice. In the 2021 report of the current RICA designated Judge, Justice Nkabinde, to the parliament (2021 report of the current RICA designated judge), it is stated that the application for an interception order must always identify the surveillance subjects or their cell phone number which is then verified with the CSPs.¹²⁷⁹

While it may be difficult to ascertain which LEO will execute the order, the identification of the surveillance subject must not be made optional in the law regulating communications surveillance. If the person is not identified, the communications surveillance order may be used on persons that are unconnected to the surveillance. It may even be reused on another person after the surveillance has been executed. The optional identification of the subject of surveillance leaves room for abuse of the process and should be avoided in Nigeria.

Nevertheless, if there are special situations in which the surveillance subject cannot be identified, the judge should decide the most effective way to execute the surveillance in a manner that prevents abuse. Optional identification of the surveillance subject in applications for an interception order should not be the norm. The judge

¹²⁷⁷ *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg v Minister of Police* 2022 (1) BCLR 46 (CC) par [203]; *Gartner v Minister of Finance* 2014 (1) BCLR 38 (CC) par [47]; *Dawood v Minister of Home Affairs*; *Shalabi v Minister of Home Affairs* 2000 (8) BCLR 837 (CC) par [52].

¹²⁷⁸ S.16(1)(a)(i) and (ii) of 70 of 2002.

¹²⁷⁹ Report of the current RICA designated judge to parliament, par [56].

must also be empowered to review the process to ensure adherence to the necessary safeguard for exceptional cases.

The application for an interception order must also specify the ground for the application and “contain full particulars of all the facts and circumstances” concerning the allegation.¹²⁸⁰ Designated judges can also demand further information as they deem fit.¹²⁸¹ The application must state whether there is a previous surveillance order or an ongoing surveillance process and applicants must provide reasons why they believe that the surveillance will produce the required evidence with proof of why they think the surveillance procedure is likely to succeed. These provisions are good examples for Nigeria to emulate because the authorising body will be empowered to access all information regarding the application and the decision is not based solely on what the applicant provides. Also, they enable an application to be considered properly before it is presented to the authorising body.

Section 16(5) of the RICA provides that an interception order may only be authorised if the designated judge is satisfied, based on the facts provided in the application, that there are reasonable grounds for surveillance to be executed. Unlike the LICR, TPPA and the CPPA, the RICA specifies the information that an application for surveillance order should contain.¹²⁸² The judge then considers the application based on the guidance provided in the RICA. In this way, the RICA ensures that the judge does not have unlimited discretion when authorising surveillance orders. The provisions detailing the content of an application guide the judge on information that must be considered in order to determine whether an application is reasonable. The RICA’s procedural guidelines are a good example for Nigeria subject to the exclusion of the two provisions discussed below.

Firstly, section 16(5)(e)(i) and (ii) of the RICA exempts the application of communications surveillance from stating if alternative procedures have been used. This exemption is applicable to investigations involving organised crimes or one into the properties acquired from the proceeds of a serious crime. LEAs may be encouraged to utilise communications surveillance even when other investigative procedures will succeed, thereby enabling unnecessary communications surveillance.

¹²⁸⁰ S.16(2)(c) of 70 of 2002.

¹²⁸¹ S.16(7)(b) of 70 of 2002.

¹²⁸² S.16(2) of 70 of 2002.

Also, the RICA does not align with section 36(1)(e) of the South African Constitution that requires an inquiry into whether there are less restrictive means of achieving the purpose of the limitation of a right.¹²⁸³ Nigerian legislation must include a provision that the authorising body must inquire into the possibility of an alternative method which is less invasive of human rights.

Secondly, section 16(6) of the RICA does not require that the judge provide reasons for the decision. In the event of a review, the judge's reasoning for the decision cannot be ascertained. Also, it cannot be verified that the judge undertook a proportionality evaluation when considering the application. It is therefore important that Nigerian legislation state clearly that the authorising body must provide reasons for its decision on communications surveillance orders as this will aid transparency.

5.4.1.8 Recommendation for Nigeria on the regulation of the pre-surveillance stage of communications surveillance

For the pre-surveillance stage, it is recommended that Nigeria's statute should provide procedural rules for the authorisation of a communications surveillance order that are clear, transparent and precise. Most importantly, the procedural rules must effectively safeguard the communications surveillance process against abuse and empower the judge to be able to ensure adequate protection of human rights. The rules must also ensure that LEAs and the authorising body do not have an unlimited discretion and should enhance objective judicial decisions on communications surveillance orders.

To achieve the aforementioned outcome, the following provisions are recommended. Firstly, the proposed statute must provide that an application for communications surveillance must identify the surveillance subject or provide reasons why such identification should be waived. It must also stipulate that the authorising body must provide additional safeguards for the right to privacy where there is a justification for a waiver of identification of surveillance subject. Furthermore, the statute must make provision for review of the process by the same authorising body who ordered the waiver of identification of the subject of surveillance.

¹²⁸³ Chapter 3, sec.6.7; *Law Society of South Africa v Minister for Transport* 2011 (1) SA 400 (CC) par [47]; Rautenbach 2005 *JSAL* 634; Rautenbach 2014 *PELR* 2233; Cohen-Eliya and Porat *Proportionality and Constitutional Culture* (2013) 111-113.

Secondly, the statute must state exactly what information must be included in an application for a communications surveillance order. This information must include evidence justifying the basis for suspicion of the surveillance subject in the alleged activity that forms one of the legitimate aims for surveillance. Also, the application must be supported by proof indicating the basis for believing that the surveillance subject has information regarding the activity that prompted the request for surveillance. Additionally, the information supporting the application must be given under oath and signify the specific information that the surveillance is expected to provide. This supporting information must provide a factual basis for a reasonable suspicion that the surveillance subject is involved in an activity linked to a legitimate aim that can prompt surveillance. The authorising body must also be empowered to request additional information when necessary.

Thirdly, the proposed statute must state specifically that the authorising body must conduct a proportionality analysis between the right to privacy and the purpose of communications surveillance. The reasoning underlying the decision must also always be provided. Also, the proposed statute must specify that the authorising body must possess full access to all information concerning the application as this will aid the proportionality exercise. The proportionality analysis must include an inquiry into why alternative methods of investigation are not utilised.

Lastly, the proposed statute should specify that an application for a surveillance order must identify the surveillance subject except in cases where it is impossible to do so. The judge must decide which cases fall within the exception and where identification of the surveillance subject can be waived. The judge must also review the process in order to ensure that LEAs do not abuse the exceptional situation.

5.4.2 The problems with the implementation stage of communications surveillance in Nigeria

The Nigerian legal framework on communications surveillance lacks an oversight mechanism on the implementation of communications surveillance. None of the laws on communications surveillance provide any procedural rules for the execution of a surveillance order. The LICR has some provisions that compel CSPs to permit communications surveillance on their network, failing which, they will be

sanctioned.¹²⁸⁴ Even though the communications surveillance order is addressed to CSPs, the LICR is unclear whether the order must be executed by CSPs or LEAs. Regulation 15(2) of the LICR provides that:

“The execution of such warrant may where required by any of the parties [LEAs] stated in paragraph (1) of this regulation, take place in the presence of the Licensee or person who manages the facilities of such Licensee.”

The most probable action is that the LEAs execute the communications surveillance order and the assistance of the CSPs is optional. This is because Regulation 15(2) provides that CSPs may be present during the execution of the order. As a result, the CSPs control whether the LEAs adhere to the specific judicial orders.

The inability of the CSPs to verify the communications surveillance order may be a way of preserving the integrity of the criminal justice procedure. This is because a CSP can leak surveillance process as they do not possess the same expertise and training in handling classified information compared to LEAs. Nevertheless, the LEAs have unfettered powers to execute communications surveillance orders. LEAs can manipulate the technical procedure of the implementation of a communications surveillance order to surpass the scope of the authorisation. **There is a lack of oversight for the implementation stage of the surveillance process by the legislature and the judiciary.**

It is acknowledged that the CSPs are required to submit a monthly report to the NCC about the communications surveillance order executed on their networks.¹²⁸⁵ However, CSPs are not required to provide details of this execution nor are they required to possess a copy of these warrants. Also, the NCC is an organ of the State just like LEAs. Consequently, the NCC does not possess independent supervisory powers over LEA activities and there is inadequate protection for the right to privacy of surveillance subjects during the implementation of a communication surveillance order by virtue of a lack of an independent oversight mechanism.

Another problem is that none of the laws refer to the existence of any technical document that stipulates the procedure for the execution of communications surveillance. This may be because the documents, if any, contain details of the surveillance procedure. The public accessibility of such documents may jeopardise

¹²⁸⁴ Regulation 15(2) and (3) of the LICR; S.147 of the Nigerian Communications Act, 2003.

¹²⁸⁵ Regulation 15(3) and (4) of the LICR.

the surveillance process. Nevertheless, these documents ought to be submitted to the legislature and the judiciary for scrutiny. This will enhance the transparency of the surveillance process and improve the safeguards against abuse. In addition, the judge presiding over a surveillance matter needs to possess full access to these technical documents to be well-informed when making communications surveillance orders.

Lastly, the CPPA and the TPPA do not provide for duration of the surveillance and a LEO can execute surveillance indefinitely. This omission is an unjustifiable limitation on the right to privacy of the surveillance subject. Even though the LICR provides that a communications surveillance order is valid for three months, it does not provide any duration for the acquisition of metadata. The LICR therefore infringes the right to privacy of a surveillance subject unjustifiably in relation to the acquisition of their metadata.

International law does not have any specific provision on the execution stage other than the broad provision already stated in section 5.4.1.4 above. The next sub-section therefore discusses the requirement of the European regional law in this respect, followed by the South African jurisprudence.

5.4.2.1 European regional law standard on communications surveillance

The scrutinization of the Russian law on communications surveillance by the ECtHR has shown the length to which LEAs can go when they have unrestrained access to communications surveillance. Evidence tendered by the applicant in *Zakharov v Russia* indicates that LEAs in that case illegally intercepted private communications of politicians and businessmen and sold the information obtained to their rivals.¹²⁸⁶ The ECtHR declared that the possibility of unlawful activities of LEAs is the reason why judges presiding over surveillance matters must possess supervisory powers over the implementation process.¹²⁸⁷ This supervisory power includes LEAs reporting the result of the surveillance to the judge who will review the implementation process to ensure compliance with all orders.¹²⁸⁸

¹²⁸⁶ *Zakharov v Russia* par [197].

¹²⁸⁷ *Zakharov v Russia* par [274]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [276].

¹²⁸⁸ *Zakharov v Russia* par [274]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [276].

The ECtHR also stated that there must be regulations that are publicly available indicating the scope of supervision of the implementation process, the conditions under which surveillance can be implemented and the review procedure.¹²⁸⁹ Additionally, laws regulating communications surveillance must clearly state the remedies available for “breaches detected” during the surveillance process.¹²⁹⁰ The ECtHR emphasised that the oversight mechanism need not be a judicial officer, but must be someone independent.¹²⁹¹ In this regard, in *Klass v Germany*¹²⁹² the ECtHR declared that the German’s legal framework (the G 10 Act)¹²⁹³ that uses an independent and external non-judicial panel, known as the G10 Commission, as the oversight body, was sufficient to safeguard rights.

The G 10 Act provides for the appointment of an intermediary who is qualified to be a judge to supervise the execution process.¹²⁹⁴ This intermediary obtains the information from the CSPs and provides the LEOs with information that is deemed useful for the investigation on which communications surveillance was ordered. Information that is not useful is destroyed immediately. LEOs therefore have no direct access to CSPs networks or the entire communications of a surveillance subject. This is a good procedure for Nigeria to follow as it will provide an independent and external supervision for the execution of the communications surveillance order. The appointment of the intermediary for Nigeria must also be devoid of influence from the Executive.

There are five lessons that can be drawn for Nigeria’s proposed new statute from the ECtHR’s assessment of both the Russian and German communications surveillance regime. Firstly, the proposed statute must contain an implementation procedure. It must clearly state who the person is to whom the judge must address the communications surveillance order, where surveillance is to take place, who is authorised to implement the surveillance order and the procedure to follow when the information is obtained. Secondly, while it is not necessary that the proposed statute

¹²⁸⁹ *Zakharov v Russia* par [276].

¹²⁹⁰ *Ibid.*

¹²⁹¹ *Zakharov v Russia* pars [277-278].

¹²⁹² *Klass v Germany* par [258]; *Weber and Saravia v Germany* par [115]; *Kennedy v United Kingdom* par [31]; *Dumitru Popescu v Romania* (no. 2), App. No. 71525/01, (2007) par [71].

¹²⁹³ Act of 13 August 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, post under Fernmeldegeheimnisses, “the G 10” Act).

¹²⁹⁴ Article 1(7) of the G 10 Act; *Klass v Germany* par [75].

contain the technical details of this procedure, it must state that LEAs must follow this process.

Thirdly, the technical documents for implementation of the surveillance must be available to the persons in charge authorising surveillance. Fourthly, LEAs must be compelled to report the result of surveillance to the judicial officers who authorise the surveillance. Lastly, an independent intermediary should be appointed who will execute the communications surveillance order and provide LEOs with the information that is relevant to their investigation only.

5.4.2.2 South African approach on the implementation of communications surveillance

The RICA establishes the Office for Interception Centre (OIC) and empowers it to maintain a direct connection with CSP networks for executing communications surveillance orders.¹²⁹⁵ Once a judicial officer authorises communications surveillance, the LEAs inform the CSP concerned and then requests that the content of communications and/or its metadata should be transferred to an interception centre.¹²⁹⁶ Thereafter the staffs of the interception centres, who are also LEOs designated to the interception centres, will execute communications surveillance based on the interception order.¹²⁹⁷ The RICA empowers the designated judge to supervise the process by demanding reports of the progress of the surveillance and adjusting the communications surveillance order as required.¹²⁹⁸ Nigeria's statute should include these provisions. In addition, the applicant for the communications surveillance order must provide a routine report, preferably monthly, detailing the progress of the surveillance. This will enable the judge to verify compliance with the order.

However, the RICA does not provide adequate safeguards against the abuse of communications surveillance, for the following reasons: Firstly, there is no provision restricting LEA access to the communications of the surveillance subject that are not necessary for the investigation. The Constitutional Court in *AmaBhungane* declared these to be "B disclosures" and excessive access and therefore unjustifiable.¹²⁹⁹ The

¹²⁹⁵ S.32 of 70 of 2002.

¹²⁹⁶ S.32 (1)(a) of 70 of 2002.

¹²⁹⁷ S.35(1)(e) of 70 of 2002.

¹²⁹⁸ S.24 of 70 of 2002.

¹²⁹⁹ *AmaBhungane v Minister of Justice* (CC) pars [122-128].

Court declared that access to the surveillance subject's communications should be limited to what is necessary for the specific investigation for which the authorisation was granted.¹³⁰⁰ This also includes communications of lawyers and journalists which may affect the right to a fair hearing of their clients and sources and which requires additional safeguards. This was discussed in detail in chapter three.¹³⁰¹

The Constitutional Court specifically upheld the applicant's argument for an intermediary and declared that the designated judge should have full access to information. This intermediary will be expected to prevent the disclosure of information that is not related to the investigation listed in the communications surveillance order.¹³⁰² Designated judges should decide, based on the evidence, whether an intermediary is necessary or provide other precautions that they deem necessary.¹³⁰³ In chapter three, it was shown that an intermediary contributes a risk to the integrity of the investigation because more people are involved.¹³⁰⁴ The risk can however be mitigated by ensuring that the persons involved in the execution process have been trained in handling classified information. Also, the number of persons involved in the process may be limited depending on the nature of investigation. Nonetheless, the protection of the surveillance subjects' right to privacy must be of paramount importance, also considering that the subject is innocent until proven guilty.

Secondly, the current report of the designated judge, which was discussed in chapter three, raised an issue regarding the independence of the OIC. In her report to parliament, Justice Nkabinde stated that these centres have "technical deficiencies" and are ineffective in executing the surveillance orders.¹³⁰⁵ According to her, a better safeguard against abuse would be if the Director of the OIC is independent from the executive and reports directly to parliament.¹³⁰⁶ Also, interception centres are not equipped to intercept social media platforms and so do not provide services to LEAs in this respect. It is submitted that interception centres, if independent and well-equipped, can serve as the intermediary between LEAs and the communication of the surveillance subject. This aspect is expanded upon below.

¹³⁰⁰ *Ibid.*

¹³⁰¹ Chapter 3; sec.3.8.2.5.5.

¹³⁰² *AmaBhungane v Minister of Justice* (CC) par [127].

¹³⁰³ *Ibid.*

¹³⁰⁴ Chapter 3; sec.3.8.2.5.5.

¹³⁰⁵ 2021 report of the current RICA designated judge par [49].

¹³⁰⁶ 2021 report of the current RICA designated judge par [49].

The current Nigerian legal framework on communications surveillance does not provide for interception centres as the execution occurs at the CSP facilities. LEAs have direct access to CSPs' networks when executing communications surveillance.¹³⁰⁷ The execution procedure, is therefore, subject to undesirable disclosure and LEAs can even obtain more information than is required or authorised. An intermediary is a necessary recommendation for safeguarding the surveillance subject's right to privacy by preventing over-disclosure of the surveillance subject's communication.

5.4.2.3 Recommendation for Nigeria on the implementation of communications surveillance

The proposed statute must state clearly that the authorising body presiding over surveillance must have access to all relevant information concerning the surveillance. The statute must set out the implementation procedure in clear and precise language, and in detail. The actual implementation technique does not need to be stated, but it must be available to the legislature and the supervisory body. The proposed statute must provide for the existence of the document containing the implementation techniques of the surveillance.

Also, an intermediary will assist in protecting information that relates to legal privilege or a journalist's source. It is recommended that the proposed statute provide for an independent intermediary who reports to the designated judge and submits an annual report to the parliament. Instead of an "Office for Interception Centres" as established by the RICA, Nigeria's proposed statute should provide for an "Office for Surveillance Intermediary". This Office should consist of legal practitioners, media persons and information and communications technology (ICT) experts. Legal practitioners and journalists have the requisite training to identify information that is protected by legal privilege and journalists' sources respectively. The ICT experts will assist in using surveillance equipment to extract useful information.

5.4.3 The post-surveillance stage of communications surveillance in Nigeria

The post-surveillance stage involves the processing of the information acquired from communications surveillance. This information is referred to as post-surveillance information and its processing includes storage, examination, assessment, usage,

¹³⁰⁷ Regulation 15(2) of the LICR.

transfer and destruction. The CPPA provides that metadata must be stored by CSPs for two years but there is no provision relating to the duration of the storage of the content of communications.¹³⁰⁸ The TPPA empowers a judge to order CSPs to retain post-surveillance information communications relating to a surveillance subject that is transmitted on their network, but it does not state the duration for which the communications must be stored.¹³⁰⁹

The LICR provides that the Authorised Agency shall destroy the intercepted communications after the completion of the investigation.¹³¹⁰ Confusingly, it also provides that the Authorised Agency can store the intercepted communications for three years.¹³¹¹ It is not clear whether the three years commences after the investigation is completed or after the information is acquired. In addition, the LICR provides that intercepted information that is not admitted into evidence during criminal proceedings must be destroyed.¹³¹² The LICR further provides that any post-surveillance information that is irrelevant to the investigation must be destroyed upon extraction.¹³¹³ This is a sound provision, provided that there is an intermediary to supervise the procedure. In the absence of such a provision, there will be not much reason to dissuade LEOs from acquiring more information than necessary. These provisions only relate to the storage and destruction of post-surveillance information. There are no provisions regarding transfer and access of post-surveillance information.

There are also a few problems with the LICR's provisions on the storage and destruction of intercepted communications. First, the provision regarding the duration of the storage of intercepted communication is unclear. Secondly, the period of investigation can be indefinite and, there is no protection to prevent abuse of the use of the information through a prolonged investigation. Thirdly, the LICR enables LEAs to extract information during communications surveillance that is irrelevant to the investigation, constituting an unjustifiable limitation of the right to privacy. Such

¹³⁰⁸ S.38 of the CPPA.

¹³⁰⁹ S.39(2)(a) of the TPPA.

¹³¹⁰ Regulation 6(1) of the LICR.

¹³¹¹ Regulation 6(3) of the LICR.

¹³¹² Regulation 6(2) of the LICR.

¹³¹³ Regulation 6(4) of the LICR.

extraction does not serve any of the legitimate aims in section 45(1) of the 1999 Nigerian Constitution and should be prohibited.

5.4.3.1 European regional law standard on the post-surveillance stage of communications surveillance

The European regional law provides solution to overcome these problems. In *Zakharov v Russia*, the ECtHR held that the Russian legal framework provides adequate safeguard to the right to privacy in respect of post-surveillance processing of information. The ECtHR confirmed that laws must provide clear and specific rules governing post-surveillance information.¹³¹⁴ The rules must provide for storage of the information under conditions that eliminate the risk of unauthorised access. This may include access for LEOs with high security clearance only. For example, the Russian law provides that information obtained from communications surveillance is “classified information” and must be handled with the same security clearance as required for all “classified information”.¹³¹⁵

The Russian law requires LEOs to be trained in data protection and handling of classified information before stored information can be released to them.¹³¹⁶ Also, the information released to these LEOs must be sufficient to perform their duties and nothing more.¹³¹⁷ Information about a surveillance subject who has not been charged for any criminal offence must be destroyed within six months of its acquisition.¹³¹⁸ This provision is clear and specific and is recommended for Nigeria’s proposed statute.

Furthermore, the ECtHR declared the Russian law that provides that only persons who are “qualified to work with classified information” and who are trained in data protection should be permitted to access post-surveillance information as adequate for the protection of the right to privacy.¹³¹⁹ It took into account that security clearance will be required to access post-surveillance information.¹³²⁰ This aspect of the judgement is not supported for the Nigerian context because the persons authorised to have

¹³¹⁴ *Zakharov v Russia* par [253]; *Kennedy v United Kingdom*, par [162-163].

¹³¹⁵ S.5(4) of the Russian State Secret Act of Law no. 5485-I, 21 July 1993; *Zakharov v Russia* par [52].

¹³¹⁶ Ss.16, 17 and 27 of the Russian State Secret Act; Regulation no. 63 of 6 February 2010 of the government of the Russian Federation par [7, 11 and 21]; *Zakharov v Russia* par [55-58].

¹³¹⁷ *Zakharov v Russia* par [57]; S.25 of the Russian Secret Service Act.

¹³¹⁸ *Zakharov v Russia* par [65]; S.5(7) of the Operational-Search Activities Act of 12 August 1995 (no.144-FZ).

¹³¹⁹ *Zakharov v Russia* par [55].

¹³²⁰ *Zakharov v Russia* par [56].

discretionary power for access and transfer of post-surveillance information are LEAs who do not possess the requisite independence to act as an oversight mechanism. This means that ultimately the State has unrestricted access to post-surveillance information.

Unlike other classified information, post-surveillance information is usually required for a criminal investigation and prosecution. As the State is also usually a party to criminal prosecutions, it is recommended that to protect the surveillance subject's right to a fair trial, it is a better practice to ensure that the State does not have unrestrained discretionary power to the access and transfer of post-surveillance information.

In *Zakharov v Russia*, the ECtHR also held that laws must ensure that non-relevant information be destroyed upon extraction, because its retention cannot be justified under article 8 of the ECHR.¹³²¹ The Court, however, condemned the excess discretion that Russian law provides to trial judges regarding the processing of information tendered in evidence.¹³²² This law provided that judges have the discretion to determine the processing of post-surveillance information that is tendered in evidence for criminal trial.¹³²³ That is, trial judges can determine the storage, transfer and destruction of the information both during and after the trial. There is no provision in the Russian legal framework on the duration for storage of information or when it must be destroyed (or how it should be transferred if necessary). An omission of this type must be avoided in the Nigerian proposed statute.

On the issue of transfer and access of information between LEAs, the ECtHR declared that the procedure for transfer must be clear.¹³²⁴ The persons in charge of the process must be clearly mentioned in the law.¹³²⁵ Also, the mechanism for transfer and access of information must eliminate the risk of inordinate disclosure.¹³²⁶

A sound law should provide for destruction of information after the LEA that applies for the surveillance has completed its investigation. Any further transfer must be determined by the surveillance judge under an application to use surveillance information. To ensure a fair hearing regarding the use of the surveillance information,

¹³²¹ *Zakharov v Russia* par [255]; *Klass v Germany* par [52]; *Kennedy v United Kingdom*, par [162].
¹³²² *Zakharov v Russia* par [66]; Article 8(3) of the Russian Code of Criminal Procedure of 18 December 2001 (No.174-EZ), in force since 1 July 2002 (CCrP).

¹³²³ *Ibid.*

¹³²⁴ *Zakharov v Russia* par [233].

¹³²⁵ *Ibid.*

¹³²⁶ *Ibid.*

an independent third party should be appointed, as surveillance subjects cannot defend themselves in court. Here, the Russian law which provides that persons who process post-surveillance information should have the security clearance to work with classified information and be qualified in data protection, is a sound example for Nigeria to the extent that such persons are independent.

5.4.3.2 South African approach on the post-surveillance stage of communications surveillance

Sections 35(1)(f) and (g) and 42 of the RICA provides for the processing of personal information. This was discussed in detail in chapter three where it was also stated that the Constitutional Court declared provisions in the RICA regarding processing of post-surveillance information unconstitutional. The proposed legal framework for Nigeria cannot emulate the RICA in this regard, however, it can benefit from the Constitutional Court's decision in *AmaBhungane*. The South African approach to processing of post-surveillance was declared unconstitutional because it was vague. Specifically, section 35(1)(f) and (g) of the RICA merely provide for the duties of the Director of the OIC, which include keeping records of post-surveillance information and prescribing the mode of usage and duration of storage of the information. The RICA should have detailed the mode of access and transfer of post-surveillance information, the destruction of relevant and irrelevant information and its storage.

The RICA provides that the post-surveillance information can be stored for a maximum period of five years. It however gives an excessive discretion to the Director of the OIC to determine when such information should be destroyed. This means that if the investigation concerning a surveillance subject is concluded within three months, the post-surveillance information can be stored for up to five years even if this information serves no purpose. The Constitutional Court held that the retention of such vital information ought not to be left to the discretion of the Director and should be regulated in the RICA.¹³²⁷ Consequently, the RICA's regime for protecting post-surveillance information provided inadequate safeguards for the right to privacy and was therefore held to be unconstitutional.¹³²⁸

¹³²⁷ *AmaBhungane v Minister of Justice* (CC) par [103].

¹³²⁸ *AmaBhungane v Minister of Justice* (CC) par [108].

As discussed in chapter three, the provisions of POPIA may be applied to ameliorate the inadequacies in the RICA in matters that do not involve national security issues. This is because section 6(c) of the POPIA exempts matters regarding national security from its ambit. Post-surveillance information that qualifies as private facts under the common law and that is exempted from the POPIA may be actionable under the common law. The common law can protect infringements to the right to privacy to the extent that legislation does not.¹³²⁹ Neither the POPIA nor the RICA provide relief for unlawful processing of post-surveillance information. Hence, the common law may provide delictual damages to be claimed by the surveillance subject for the wrongful use of post-surveillance information, albeit for private facts alone.¹³³⁰

The lack of adequate provision for the processing of post-surveillance information in the RICA means solutions are needed elsewhere, that is in the POPIA and the common law. While these other laws provide some relief, there are still gaps that should be rectified by clear and specific provisions on the processing of post-surveillance information in the RICA. Nigeria's proposed statute must, therefore, avoid the problems in the RICA. It is recommended that the proposed statute provide clearly for the processing of post-surveillance information and in a manner that adequately safeguards the right to privacy.

5.4.3.3 Recommendation for the post-surveillance stage of communications surveillance

It is recommended that the procedure for post-surveillance information be clearly stated in the proposed statute. The proposed statute must provide for someone who is responsible for handling post-surveillance information, that is, the particular office must be stated. For example, the RICA designates the Director of the OIC for this purpose, which is a good example of a clearly designated authority being placed in charge of post-surveillance information. It must, however, be noted that the Director of OIC does not possess independence because s/he is an appointee of the President.

¹³²⁹ S.8(3) of the South African Constitution.

¹³³⁰ Chapter 3, section 7.1; Invasion of privacy under delict is actionable where private facts are concerned. *De Klerk v Minister of Police* 2020 (1) SACR 1 (CC) par [122]; *Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 (3) SA 56 (W) 60; Neethling *et al Personality Rights* 49; McQuoid-Mason *The Law of Privacy in South Africa* (1978) 37-39, 86-88; Neethling *et al Law of Delict* 422.

It is therefore suggested that the proposed statute establish an office that is independent from the executive, which can be supervised by the judiciary and reports to the legislature.

The “Office for Surveillance Intermediary” (OSI) as recommended above is also useful for this purpose. It is in the interest of a surveillance subject’s rights to a fair trial and a fair hearing, that a legally trained third party acts as an intermediary and be in charge of determining the processing of post-surveillance information. This does not mean that the intermediary will have excessive discretion, but that he or she will be able to monitor the non-arbitrary use of post-surveillance information.

The proposed statute should provide that post-surveillance information may be stored for a period of three years and this must be subject to constant supervision, preferably annually, to justify the continued storage within the prescribed period. The statute must also set out the procedure for extension of the prescribed period of storage, which must include LEAs justifying why the investigation is not concluded. Also, post-surveillance information must be used strictly for the legitimate aims as stipulated in section 45(1) of the 1999 Nigerian Constitution. Where there is no notice of appeal, the statute must stipulate that trial judges must destroy post-surveillance information after one month where there is no notice of appeal. Otherwise, the judge must give reasons why post-surveillance information should be stored for longer than one month.

In order to ensure that LEAs use post-surveillance information for legitimate purposes, it is recommended that the transfer of information between LEAs must be authorised by a judge in the same way as a surveillance order is issued. Hence inter-governmental transfer of surveillance information must be supervised. In addition, the proposed statute must provide that post-surveillance information should be handled in a similar way to “classified information” with the persons processing post-surveillance information having experience in data protection.

5.5 Independent and effective oversight mechanisms for communications surveillance

5.5.1 The problem with the oversight mechanisms for communications surveillance

The laws regulating communications surveillance in Nigeria provide for judicial authorisation of communications surveillance, but at the pre-surveillance stage only.

As discussed in section 5.4.2 and 5.4.3 above, there is no oversight body monitoring the implementation and post-surveillance stages of communications surveillance. Recommendations to address this problem are also provided above. An independent and effective authorisation process is important.

However, there is also a need for judicial supervision of the implementation and the post-surveillance process. An independent and effective authorisation process is important and will ensure accountability. If the authorisation stage of communications surveillance fails to have regard for human rights, the supervisory mechanisms in the other stages will be ineffective as they only implement the communications surveillance order. The problems with the oversight mechanism for the communications surveillance regime in Nigeria are as follows:

Firstly, judges do not have full access to all the information relating to the communications surveillance applications. Sections 39(1) of the CPPA and 13(3) of the TPPA provide that a judge may authorise communications surveillance based on information on oath. Sections 13(3) of the LICR and 29(1) of the TPPA have similar provisions, but do not require the information supporting the application to be under oath. These laws do not empower judges to request further information concerning the application. The decision of the court is based solely on the information provided by the LEO, who may withhold unfavourable information. Judges may therefore be unable to consider all relevant information regarding the application and to give adequate safeguards to the surveillance subject.

Secondly, the laws provide that the authorisation of a communications surveillance order is heard as an *ex parte* application. Ordinarily, Nigerian courts require the parties to an *ex parte* order, to report to court on an appointed date before the Court finalises the orders. This enables the party on whom the orders are served to dispute the facts or law on which the *ex parte* application was granted.¹³³¹ Surveillance applications in Nigeria, are however, unlike other *ex parte* applications, because none of the laws regulating communications surveillance provide for service on the application on the surveillance subjects. Hence the surveillance subjects are unable to dispute the application. This is problematic and constitutes an infringement of the rights of access to court and a fair hearing of the surveillance subject.

¹³³¹ Order 43(3) Lagos State High Court (Civil Procedure) Rules 2019.

It also means that surveillance subjects will be unable to represent themselves at the authorisation stage of the surveillance process. There is thus no opportunity for surveillance subjects to be heard, thereby eroding their right to a fair hearing. It is understood that communications surveillance requires secrecy of the process in order to be effective, but the right to a fair hearing of the surveillance subject must be protected.

Lastly, there are no reports on the number of communications surveillance applications granted or denied, impacting on transparency. There is also no way of assessing whether judges scrutinise the applications or just rubber-stamp them. As a result, the effectiveness of the oversight function performed by judges cannot be assessed. Reform is therefore needed.

5.5.2 International law on instituting oversight bodies

International law requires that domestic laws regulating communications surveillance must have an independent and external oversight body that monitors the activities of LEOs.¹³³² The judiciary is the preferred oversight body if it conforms with international standard for independence. “Judicial involvement” in communications surveillance must also be transparent and impartial and it should not be viewed as a definitive solution.¹³³³ Here, the report of the OHCHR is important. It recorded that judicial authorisation of communications surveillance orders in many of the Member States has “amounted effectively to an exercise in rubber-stamping”.¹³³⁴ A mixed method of oversight over communications surveillance was thus proposed. This involves administrative, judicial and parliamentary oversight bodies, independent from State interference.¹³³⁵

The Nigerian legal framework lacks external monitoring of the surveillance implementation procedure and a post-surveillance review process. For the external monitoring procedure during implementation, the Nigerian framework needs an independent administrative oversight body. It should also require judges to embark on a review process after the surveillance is completed and provide an annual report to be submitted to parliament. This report should include the number of communications

¹³³² 2014 OHCHR Report, par [38].

¹³³³ *Ibid.*

¹³³⁴ *Ibid.*

¹³³⁵ *Ibid.*

surveillance orders granted and the challenges encountered to enable parliament to resolve the problems.

5.5.3 Regional law on instituting oversight bodies

African regional law is used to determine the African law benchmark for the oversight body on communications surveillance among Members of the African Union. This will serve to recommend reforms for the current Nigerian legal framework. The European regional law is discussed to extract concrete recommendations for Nigeria.

5.5.3.1 African regional law on instituting oversight bodies

The 2019 Declaration requires laws of Member States to provide “prior authorisation of an independent and impartial judicial authority”.¹³³⁶ This signifies that the AU mandates Member States to select judges as the authorisation body for communications surveillance.¹³³⁷ There is however no provision in the 2019 Declaration for an independent oversight body for the implementation stage and the post-surveillance stage.¹³³⁸

Although, it is expected of Member States to institute judicial oversight at the pre-surveillance stage, the underlying principle is that the oversight body be independent from the executive. It is, therefore, unlikely that a Member State that opts for a non-judicial panel that is independent and which effectively ensures protection of human rights, will be deemed not to have complied with the 2019 Declaration. This is important because the next sub-section recommends a non-judicial panel for Nigeria, which is drawn from Germany’s oversight approach to communications surveillance. An issue, however, is that the 2019 Declaration is not binding on Member States and it may be difficult for the African Union to compel compliance.¹³³⁹

5.5.3.2 European regional law on instituting oversight bodies

Section 5.4 above discusses the ECtHR’s recommended minimum safeguards for effective procedural supervision of the oversight bodies. In this section the ECtHR’s analysis of the Bulgarian, Russian and German laws in relation to their oversight

¹³³⁶ Principle 41(3)(a) of the 2019 Declaration.

¹³³⁷ *Ibid.*

¹³³⁸ Principle 41 of the 2019 Declaration.

¹³³⁹ Special Rapporteur in his introduction to the 2019 Declaration referred to the document as a “soft law”.

mechanisms is used to recommend reforms for Nigeria, as the ECtHR evaluated the oversight bodies of these countries extensively.

The ECtHR held in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* that the duty of the court as the independent oversight body is to ensure that there are substantial safeguards against arbitrary and indiscriminate surveillance.¹³⁴⁰ It emphasised that this oversight function involves an independent and external supervision at all stages of the surveillance process.¹³⁴¹ Because the Bulgarian communications surveillance laws did not provide an oversight mechanism for the execution and post-surveillance stage, the ECtHR declared the Bulgarian oversight mechanism, ineffective to safeguard rights.¹³⁴²

In assessing the effectiveness of the Russian judicial authority to provide adequate safeguards, the ECtHR held that the duty of the court is to “ascertain” whether the request for communications surveillance is “necessary in a democratic society” as provided in article 8(2) of the ECHR.¹³⁴³ It also stated that the court must evaluate whether the intended surveillance is “proportionate to the legitimate aim pursued.”¹³⁴⁴ This includes the court assessing whether there are less restrictive means to achieve the aim.¹³⁴⁵

The ECtHR further declared that courts are unable to embark on the proportionality exercise effectively if they are not empowered to request information relevant to the application.¹³⁴⁶ It is especially crucial that the court be so empowered as this supports an applicant’s claim for a communication surveillance order.¹³⁴⁷ This was not the case with the Russian laws regulating communications surveillance which, like Nigeria’s legal framework, does not empower judges to request additional information.¹³⁴⁸ The

¹³⁴⁰ *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [84].

¹³⁴¹ *Ibid.*

¹³⁴² *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [85].

¹³⁴³ *Zakharov v Russia* par [260]; *Klass v Germany* par [51]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* pars [79-80]; *Iordachi v Moldova* App. no. 25198/02 (2009) par [51]; *Kennedy v United Kingdom* pars [31-32].

¹³⁴⁴ *Ibid.*

¹³⁴⁵ *Ibid.*

¹³⁴⁶ *Zakharov v Russia* par [261]; *Chahal v United Kingdom* App. No. 22414/93 (1996) par [131]; *Liu v Russia* App. no. 42086/05 (2007) par [59-63].

¹³⁴⁷ *Zakharov v Russia* par [262].

¹³⁴⁸ *Zakharov v Russia* par [263].

ECtHR thus held that the Russian oversight mechanism was inadequate to safeguard rights against abuse when utilising communications surveillance.¹³⁴⁹

To the contrary, in *Klass v Germany* the ECtHR held that, the German's oversight mechanism, consisting of a dual supervisory body namely a parliamentary body and the G10 Commission, provided an adequate safeguard against the abuse of rights.¹³⁵⁰ The G10 Commission is a non-judicial panel that authorises communications surveillance in Germany.¹³⁵¹ It consists of three members, including the chairman who "must be qualified to hold a judicial position".¹³⁵² The appointment of the members of the G 10 Commission is independent from the State, as they are appointed by the parliamentary Board.¹³⁵³

The G 10 Commission authorises communications surveillance orders and reviews the procedure through a monthly report authored by the Minister of Interior and of Defence on the status of the communications surveillance order.¹³⁵⁴ The ECtHR's approval of Germany's non-judicial supervisory panel for communications surveillance indicates that the benchmark is an independent, external and effective oversight body.¹³⁵⁵ Although the judiciary is the preferred supervisory body for communications surveillance, the ECtHR stated that the effectiveness of the oversight in protecting rights, is more important.¹³⁵⁶

Also, in *Klass*, the ECtHR held that the absence of judicial control on surveillance did not "exceed the limits of what may be deemed necessary in a democratic society".¹³⁵⁷ This is because the alternative oversight mechanism employed is independent and possesses sufficient powers to supervise the communications surveillance procedure effectively.¹³⁵⁸ Germany's oversight approach is a good example for Nigeria. It provides a structure that merges an effective supervisory control of the

¹³⁴⁹ *Ibid.*

¹³⁵⁰ *Klass v Germany* par [60].

¹³⁵¹ *Klass v Germany* par [21].

¹³⁵² Article 1 (9) of the G 10 Act; *Weber and Saravia v Germany* par [21].

¹³⁵³ *Klass v Germany* par [21].

¹³⁵⁴ *Ibid*; section 5.4.2.2 above identifies the importance of a reporting system to parliament. This is also the practice in the South African communications surveillance regime.

¹³⁵⁵ *Klass v Germany* par [51].

¹³⁵⁶ *Klass v Germany* par [56].

¹³⁵⁷ *Klass v Germany* par [56].

¹³⁵⁸ *Ibid.*

communications surveillance procedure that can accommodate expert inputs, with independence of the persons in charge of the oversight duties.¹³⁵⁹

In Germany the execution of the communications surveillance order is performed by an independently appointed intermediary, who is qualified to hold judicial office.¹³⁶⁰ This intermediary receives the order, then sifts through the surveillance subjects' communications to extract what is needed by the applicant.¹³⁶¹ Thereafter, the information that is unnecessary to the order is immediately destroyed.¹³⁶² This is a good example for Nigeria's proposed new statute, as this will ensure that execution of the surveillance orders are supervised by personnel that are independent from the executive.¹³⁶³

The oversight function in the German communications surveillance regime is also undertaken by the parliamentary board which consists of five members that must include representations from the opposition party.¹³⁶⁴ The Ministers of the Interior and Defence must provide a six-monthly report on communications surveillance to the parliamentary Board.¹³⁶⁵ This aids transparency as the activities of the executive are also monitored and scrutinised by the parliament.

5.5.4 South African approach on instituting oversight bodies

The South African legal framework on communications surveillance utilises judicial officers at the pre-surveillance stage.¹³⁶⁶ The RICA empowers the Minister of Justice to appoint a designated judge who evaluates applications for the interception of communications and real-time communication-related information.¹³⁶⁷ The designated judge must also be a retired judge or a person discharged from active duty.¹³⁶⁸

¹³⁵⁹ *Klass v Germany* par [21]; The G10 Commission is a panel of three persons. This system is flexible enough to permit an ICT expert.

¹³⁶⁰ *Klass v Germany* par [20].

¹³⁶¹ *Ibid.*

¹³⁶² *Ibid.*

¹³⁶³ This is recommended in section 5.4.2.3.

¹³⁶⁴ *Klass v Germany* par [21].

¹³⁶⁵ *Ibid.*

¹³⁶⁶ Ss.16, 17 and 18 of 70 of 2002.

¹³⁶⁷ S.1 of 70 of 2002 refers to the metadata of an electronic communication that is transmitted with 90 days as real-time communication-related information. The metadata of an electronic communication that is stored after 90 days of the transmission is referred to as archived communication-related information.

¹³⁶⁸ *Ibid.*

Archived communication-related information may, however, be authorised by any judge of a High Court, a regional court magistrate or a magistrate.¹³⁶⁹

One of the positive aspects of the RICA in respect of the authorising body is the creation of a designated judge. The designated judge is focused on surveillance matters only. This approach promotes effectiveness as the designated judge, unlike other judicial officers, will not be burdened with the day-to-day activity of the court. This resonates with the recommendation in 5.2 above that Nigeria create a tribunal that is focused on communications surveillance. Another positive example in the RICA is that designated judges are entitled to have full access to information regarding the application for communications surveillance.¹³⁷⁰ There are, however, a few problems with the South African approach, which is one of the grounds upon which sections in the RICA were declared unconstitutional.¹³⁷¹

First, the Minister of Justice who is a Member of the Executive, is responsible for the appointment of a designated judge.¹³⁷² Also, the term of office of the designated judge is not stated; neither is there any indication suggesting that the term is non-renewable. This jeopardises the independence of the designated judge as there is a possibility that the judge may be threatened with non-renewal of term or induced by the possibility of a renewal.¹³⁷³

Secondly, the archived communication-related information is handled like regular warrants by a judge, regional magistrate or magistrate.¹³⁷⁴ Judicial officers, unlike the designated judge, may neither understand the peculiarity of a surveillance order, nor have the time to request a thorough evaluation of the application. Hence, it is likely that the surveillance subjects' rights may not be adequately protected. The High Court, in highlighting the peculiarity of communications surveillance proceedings in *AmaBhungane*, held that the designated judge risks having “tunnel vision” because the judge lacks the diverse arguments that an opposing attorney will present.¹³⁷⁵ The High Court recommended that a panel of designated judges may resolve this

¹³⁶⁹ S.19 of 70 of 2002.

¹³⁷⁰ S.16(7)(b) of 70 of 2002.

¹³⁷¹ *AmaBhungane v Minister of Justice* (CC) par [94].

¹³⁷² S.1 of 70 of 2002.

¹³⁷³ *AmaBhungane v Minister of Justice* (CC) par [91].

¹³⁷⁴ S.19 of 70 of 2002.

¹³⁷⁵ *AmaBhungane v Minister of Justice* (GP) par [80].

problem.¹³⁷⁶ The Constitutional Court, however, refused to comment on the modalities of safeguards that are appropriate for the body presiding on preauthorisation of surveillance as this is a decision within the purview of parliament.¹³⁷⁷ This recommendation aligns with the approach in 5.2 above on the need for a non-judicial tribunal as the oversight body for communications surveillance.

Thirdly, the RICA does not provide any independent supervisory body for the execution of the communications surveillance order. The Constitutional Court stressed the importance of ensuring that the oversight body is independent from the executive as this will restrain any threat or inducement of the supervisory body.¹³⁷⁸ The Office for Interception Centre (OIC) which executes communications surveillance orders does not possess the requisite independence to safeguard the execution of the communications surveillance against abuse. The Director of the OIC is appointed by the Minister of Intelligence Services and reports to the same Minister.¹³⁷⁹ The various interception centres are also headed by LEOs transferred from various law enforcement agencies.¹³⁸⁰ Thus, the OIC is subject to the direction of the Minister of Intelligence Services and is therefore not independent from the Executive.¹³⁸¹

The 2021 Report of the current RICA designated judge highlights the lack of independence of the OIC.¹³⁸² The Director of the OIC recommended that the OIC should report directly to parliament as this will foster its independence.¹³⁸³ This, however, is not enough to achieve an independent oversight body for the implementation of communications surveillance as the entire internal structure of the OIC must be overhauled. The executive appointment of the Director of the OIC and the heads of interception centres is problematic. Also, the current structure in terms of which the LEOs are employees of the OIC is not ideal, independent persons should be used instead.

¹³⁷⁶ *Ibid.*

¹³⁷⁷ *AmaBhungane v Minister of Justice* (CC) par [99].

¹³⁷⁸ *AmaBhungane v Minister of Justice* (CC) par [90]; *Justice Alliance of South Africa v President of Republic of South Africa*; *Centre for Applied Legal Studies v President of Republic of South Africa* 2011 (5) SA 388 (CC) par [73].

¹³⁷⁹ S.34 of 70 of 2002.

¹³⁸⁰ S.36(1) of 70 of 2002.

¹³⁸¹ S.36(1) of 70 of 2002.

¹³⁸² 2021 report of the current RICA designated judge, par [51].

¹³⁸³ *Ibid.*

From this summary, it is clear that the South African approach towards the oversight for communications surveillance does not provide adequate safeguards for abuse and it is therefore not recommended for Nigeria.

5.5.5 Recommendation for Nigeria on instituting oversight bodies

Given that the South African approach to oversight for communications surveillance is not ideal and noting that international and African regional law provide a broad guideline, the most practical recommendations are drawn from the European regional law. First, it is recommended that the proposed statute for Nigeria provide for a non-judicial tribunal, vetted by parliament, to exercise oversight functions in relation to the communications surveillance process. This is necessary, because an effective supervision of communications surveillance requires a thorough examination of applications that may be too burdensome for judicial officers.¹³⁸⁴ It should also require the inputs of experts in ICT and surveillance law. A tribunal can be constituted to include persons with this expertise.

The tribunal should be headed by a chairman who is qualified for judicial office and who possesses expertise in the field of digital privacy and communications surveillance. The other members of the tribunal should include an ICT expert and a qualified journalist. This will ensure that special categories of persons, such as journalists and legal practitioners who have some constitutionally recognised right to confidentiality are represented.¹³⁸⁵ The OSI that was recommended in 5.4.2.3 above could be headed by a person who is qualified to hold judicial office and who will coordinate and supervise the execution of communications surveillance orders. The tribunal must also have a fixed, non-renewable term to ensure that it is free from inducement.

Secondly, this tribunal should report to a parliamentary committee on the execution of its mandate. The parliamentary committee must include members of the opposition to the ruling party in order to ensure impartiality. Thirdly, there must be a supervisory

¹³⁸⁴ Interview with the Retired Chief Registrar of the Supreme Court, Mrs Hadizatu Uwani Mustapha “With 10, 000 Pending Appeals, the Supreme Court is Overworked” (17 August 2021) *This Day Newspaper* <https://www.thisdaylive.com/index.php/2021/08/17/with-10000-pending-appeals-the-supreme-court-is-overworked/> (accessed 2021-12-01); Agbu “Worked to the Grave: Neglect of Work-Life Balance maybe Killing Judges” (9 November 2021) *Legal Business Day* <https://legal.businessday.ng/2021/11/11/worked-to-the-grave-neglect-of-work-life-balance-may-be-killing-judges/> (accessed 2021-12-01).

¹³⁸⁵ This is explained in detail in Chapter 3, sec. 3.8.2.5.3.

body equipped to execute communications surveillance orders and headed by a person who is qualified to be a judge. Section 5.4.2.3 above recommended that an OSI be created for the execution of communications surveillance. This recommendation works here too, provided the Office is equipped appropriately and has independent staff members with expertise in ICT required to execute the order effectively. The head of this office, who must be an experienced legal practitioner, will be able to interpret the surveillance orders effectively to determine the exact information required by LEOs and in turn prevent undesirable disclosures of information.

5.6 An effective avenue for redress

The legal framework for communications surveillance in Nigeria does not provide the surveillance subject with an opportunity to seek redress if an abuse of rights occurs. None of the laws, that is the CPPA, TPPA and LICR, provide that the surveillance subject should be notified after the surveillance. As a result, a surveillance subject is unable to review the process and seek redress where there has been an unlawful infringement of rights.

The TPPA and the CPPA neither permit, nor prohibit, post-surveillance notification. This is not mentioned in the statutes at all. Nevertheless, the practice is that surveillance subjects are not notified of the surveillance. The LICR specifically prohibits post-surveillance notification. The current Nigerian position is therefore that surveillance subjects are denied an avenue to seek redress. Also, there is no provision for a review of the surveillance process. This is a pity, as reviews permit scrutiny of the process to ensure that the rights of the surveillance subject are not unlawfully infringed during surveillance. The current Nigerian framework on communications surveillance needs reform in order to provide an avenue for redress and/or review of the surveillance process. The question is how this should be achieved.

5.6.1 International law standards for an effective avenue for redress

International law provides general and specific guidelines for Member States to achieve effective redress in their communications surveillance regime. Generally, article 2(3)(a) of the ICCPR provides that victims of violations of Covenant rights must have an avenue to seek an effective remedy. Article 2(3)(b) mandates Member States to:

“ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy”.¹³⁸⁶

An effective redress for human rights violations includes the investigation of an allegation of a violation and the enforcement of remedies.¹³⁸⁷ Member States have an obligation to investigate alleged violations of any of the rights in the ICCPR.¹³⁸⁸ They also have an obligation to make reparations to the victims of such violations. Redress is only effective when there is reparation to the victim of the violation and measures are taken to avoid the recurrence of the human rights abuses.¹³⁸⁹ These measures include that perpetrators be punished.¹³⁹⁰

Specifically, the 2014 OHCHR Report highlights certain characteristics of a communications surveillance regime that provides for an effective remedy. First, the remedies must be “known” and accessible.¹³⁹¹ Post-surveillance notification is the means of ensuring that surveillance subjects can be personally involved in the review process.¹³⁹² The 2014 OHCHR Report states that some Member States permit post-surveillance notification, while others do not.¹³⁹³ However, no clear position on the international standard is taken in this regard. Consequently, international law cannot guide Nigeria on whether post-surveillance notification should be mandatory or optional.

This is problematic as post-surveillance notification provides the surveillance subject with *locus standi* and enables the surveillance subject to seek redress for the unlawful infringement of their right to privacy. It will also enable the surveillance subject to challenge any laws regulating communications surveillance that are not aligned with the relevant standard. It is clear that this issue should be addressed at the international level with reference to existing treaty rights.

For example, article 2(3) of the ICCPR provides a right to seek redress, which is determined by a competent judicial, administrative or legislative authority. This can

¹³⁸⁶ (2014 OHCHR Report), par [39].

¹³⁸⁷ (2014 OHCHR Report), par [39]; General Comment 31, par [15].

¹³⁸⁸ General Comment 31, par [16].

¹³⁸⁹ General Comment 31, par [17].

¹³⁹⁰ *Ibid.*

¹³⁹¹ 2014 OHCHR Report, par [40].

¹³⁹² 2014 OHCHR Report, par [40].

¹³⁹³ *Ibid.*

only be possible when a person is aware of surveillance, failing which there is no avenue to seek redress. Mandatory post-surveillance notification, therefore, aligns with article 2(3) of the ICCPR and should be the international standard.

Secondly, an effective remedy “involves prompt, thorough and impartial investigation of alleged violations”.¹³⁹⁴ This is one of the duties of the independent oversight body. Thirdly, effective remedies “must be capable of ending ongoing violations”.¹³⁹⁵ This is tied ultimately to effective and efficient supervision of the procedure. Lastly, an effective avenue for redress must enable criminal prosecution of perpetrators where necessary.¹³⁹⁶ Perjury is one of the offences often committed by LEOs and an effective redress measure will ensure the prevention and prosecution thereof. These international law guidelines for effective redress will be used for recommendations for Nigeria’s proposed statute.

5.6.2 Regional law for an effective avenue for redress

5.6.2.1 African regional law for an effective avenue for redress

The 2019 Declaration provides a clear position on post-surveillance notification and will be recommended for Nigeria’s proposed statute.¹³⁹⁷ No provision is made for a definition for a “reasonable time” for post-surveillance notification in the 2019 Declaration. This is probably because the 2019 Declaration is merely a guideline and not a model law. Hence, Member States must determine what is considered a “reasonable time” in their context, working on a case-by-case basis. Foreign law, such as South African law and European law, that has been tested by the ECtHR, are considered next to determine the duration of a “reasonable time” in terms of post-surveillance notification.

5.6.2.2 European regional law for an effective avenue for redress

The ECtHR has addressed two recurring issues regarding an effective avenue for redress, namely *locus standi* and post-surveillance notification. The Court has held in several cases that the presence of a surveillance law signifies an infringement of the

¹³⁹⁴ 2014 OHCHR Report, par [41].

¹³⁹⁵ *Ibid.*

¹³⁹⁶ *Ibid.*

¹³⁹⁷ The 2019 Declaration provides that adequate safeguards involve notifying the surveillance subject of the surveillance. Principle 41(3)(d) states that laws authorising communications surveillance must provide “notification...within a reasonable time of the conclusion of such surveillance.”

right to privacy, and individuals affected by the law do not require proof that they are under surveillance to challenge the law.¹³⁹⁸ On post-surveillance notification, the Court has held that the absence of post-surveillance notification does not render a surveillance law inconsistent with the ECHR.¹³⁹⁹ The law must, however, provide an effective avenue to seek redress. In chapter two, the Bulgarian, UK and German surveillance regimes were assessed. The key points are summarised here.

The ECtHR in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*¹⁴⁰⁰ held that the Bulgarian law was inconsistent with the ECHR, because there was no effective avenue to seek redress, and the surveillance subject was also not notified. Post-surveillance notification was important because that was the only avenue through which the surveillance subject could seek redress by reviewing the process. The ECtHR accordingly held that the absence of a post-surveillance notification procedure deprived the surveillance subject of an avenue to seek redress.

In contrast, the ECtHR held in *Kennedy v United Kingdom*¹⁴⁰¹ that the UK's surveillance regime was consistent with the ECHR, even though it did not provide for post-surveillance notification. This is because the UK's surveillance regime provides for an oversight mechanism, that is, the Investigatory Powers Tribunal (IPT), where persons who suspect that they are under surveillance can seek redress. The ECtHR held that the UK approach was effective.

The German surveillance regime provides for both a post-surveillance notification and various avenues to seek redress. These avenues for redress include an application for a review of the process with the G 10 Commission, civil remedies for damages and challenging the law at the Federal Constitutional Court. The ECtHR in *Klass v Germany* thus declared that the German surveillance regime provides an effective avenue for redress.¹⁴⁰² This would have applied even if the post-surveillance notification was absent.

¹³⁹⁸ *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [69]; *Klass v Germany* par [41]; *Malone v United Kingdom* par [64]; *Weber and Saravia v Germany* pars [77-79].

¹³⁹⁹ *Klass v Germany* par [68].

¹⁴⁰⁰ *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* par [103].

¹⁴⁰¹ *Kennedy v United Kingdom* par [167].

¹⁴⁰² *Klass v Germany* par [72].

Chapter two detailed reasons why the German approach is preferred and recommended for Nigeria. To reiterate, the German approach provides surveillance subjects with an opportunity to review the process, of which they would otherwise have been deprived, as surveillance is executed secretly. In addition, because the African regional law mandates Member States to ensure that their surveillance laws must provide for post-surveillance notification, the German approach is in line with the African regional law and recommended for Nigeria.

5.6.3 South African approach for an effective avenue for redress

The RICA provides neither for any recourse nor post-surveillance notification. This *lacuna* was challenged successfully in *AmaBhungane*.¹⁴⁰³ The Constitutional Court held that post-surveillance notification is necessary so that surveillance subjects can review the process and seek redress where there is an unlawful interference with their privacy. It also held that post-surveillance notification will serve as a disincentive to LEOs to engage in unlawful surveillance, as there will be a possibility of challenging the procedure. To arrive at this decision, the Court considered the practice of the United States, Canada, Denmark, as well as the decisions of the ECtHR.¹⁴⁰⁴ It also held, based on foreign law, that ninety days is a reasonable time for a surveillance subject to be notified.¹⁴⁰⁵ This decision provides a specific guideline for the recommended period for post-surveillance notification, that is ninety days, and provides content to the African regional law's requirement of a reasonable time.¹⁴⁰⁶ This period is, therefore, recommended for Nigeria.

The Court noted, however, that post-surveillance notification may not provide redress for surveillance subjects who may be unable to review the surveillance process because of financial incapacity.¹⁴⁰⁷ The Court stated that an automatic review may provide a solution to this problem. The discussion in chapter three, however, highlighted the defects with the automatic review. It revealed that, while an automatic review may be recommended for the execution and the post-surveillance stages of

¹⁴⁰³ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* (CC) par [149].

¹⁴⁰⁴ This is discussed in detail in chapter 3, sec. 8.2.5.2; *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* (CC) par [46]; *Association for European Integration and Human Rights and Ekimdzhiiev v Bulgaria* par [90].

¹⁴⁰⁵ *Ibid.*

¹⁴⁰⁶ Principle 41(3)(d) of the 2019 Declaration.

¹⁴⁰⁷ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* (CC) par [49].

surveillance, it is not recommended for the authorisation stage, unless there is a separate body, other than the designated judge that will conduct the review. This is because the designated judge cannot objectively review a communications surveillance that she or he authorised. Hence, it is recommended for Nigeria that another body, preferably a judge of the High Court, review the authorisation process, while the designated judge will thereafter review the execution and the post-surveillance procedure.

5.6.4 Recommendation for Nigeria for an effective avenue for redress

There are three recommendations for Nigeria's legal framework on communications surveillance regarding an effective avenue for redress. First, the proposed new statute must provide post-surveillance notification to the surveillance subject. This should be done by the independent authorising panel after it has verified that the investigation will not be jeopardised. Secondly, it is recommended that the surveillance subject should be notified of the surveillance within ninety days of the conclusion of the surveillance. Where the independent panel is convinced that notification within the ninety days will jeopardise the investigation, then the notification can be postponed until such time as it is safe to do so. This means that the status of the surveillance will continuously be assessed to determine when the post-surveillance notification should occur.

Thirdly, an automatic review is recommended as this ensures that the surveillance process is reviewed to determine whether there was unlawfulness at any stage. While the authorising body can review the execution and the post-surveillance procedure, there must be another body, preferably a judicial officer, who will review the authorisation procedure of the communications surveillance order. To this effect, the first stage is a review to a judicial officer. When the lawfulness of the authorisation is confirmed, then the authorising body may proceed to review the execution and post-surveillance stages of the surveillance. This will ensure that judges are involved in the process only at the authorisation stage, as opposed to being the authorising body as stipulated in the LICR, TPPA and CPPA. Also, this approach ensures that the authorisation of the surveillance order is reviewed by a different body and thus resolves the issue raised in chapter three regarding the designated judge's objectivity during automatic review.

Surveillance subjects should be notified of the surveillance after the procedure and provided with the review report, while also being afforded an opportunity to challenge the procedure. A civil remedy for damages will also be appropriate where communications surveillance is unlawful. In this regard, developing a tort of privacy as recommended in chapter four will be useful for compensating the surveillance subject.

5.7 Conclusion

This chapter provided practical recommendations to address and rectify the unlawful legal framework for communications surveillance in Nigeria. The recommendations were divided into five broad headings. **The first recommendation dealt with the correct interpretation of the limitation clause, that is, section 45(1) of the 1999 Nigerian Constitution. The other four recommendations addressed the four main problematic themes as identified in chapter one namely:** a comprehensive statute on communications surveillance in Nigeria; a fair and effective procedural rule at all stages of communications surveillance; an effective oversight mechanism; and an effective avenue to seek redress.

To solve these problems, the chapter collated lessons from international, African and European regional law and the South African law on communications surveillance, that were discussed in chapters two and three. Ultimately, the objective was to recommend a new legal framework on communications surveillance for Nigeria that is tailored towards protecting human rights and minimising unlawfulness and arbitrariness.

Regarding the problem of incorrect interpretation of section 45(1), the limitation clause, it was stressed that it is important that the “reasonably justifiable in a democratic society” portion be interpreted correctly by the courts. It was highlighted that international and African regional law be used to define “reasonable” as “proportionate” and “necessary”, which means that section 45(1) must be interpreted to reflect a proportionality evaluation. It was also recommended that the definition of the legitimate aims as provided in the Siracusa Principles, should be adopted by the Nigerian Courts when conducting a proportionality evaluation of section 45(1).

The next recommendations were tailored towards the need for a new statute on communications surveillance in Nigeria. International, African and European regional law, as well as the South African law on the right to privacy and communications

surveillance, were explored with a view to recommend these reforms. However, as the guidelines for regulating communications surveillance for Member States in international and African regional law do not translate into national law that adequately protects human rights, regard was had to the European regional law, which provides clear and practical minimum safeguards for laws regulating communications surveillance. These minimum safeguards were developed by scrutinising the surveillance laws of the Contracting States of the ECHR specifically Russia, Bulgaria, the UK and Germany. The ECtHR has also developed effective procedural guidelines, useful independent and effective oversight mechanisms and an effective avenue for redress. These were used to provide recommendations for the Nigerian context.

The South African laws on communications surveillance, together with the decisions of the High Court and the Constitutional Court in *AmaBhungane*, provide many examples for Nigeria. Not only do these decisions flag the loopholes that Nigeria should avoid in the proposed new statute regulating communications surveillance, they also provide practical recommendations. These recommendations include an automatic review procedure that reflects the challenges of an African society and the prevention of undesirable disclosures of surveillance information.

The main recommendation towards ensuring that there is a comprehensive statute regulating communications surveillance in Nigeria is that the LICR should be repealed and a new statute that is focused solely on regulating communications surveillance be enacted. The provisions in other laws, such as the CPPA and the TPPA regulating communications surveillance, should be amended to refer to the new statute for the utilisation of communications surveillance. A recommended name for the new statute is the Communications Surveillance Act because its title should reflect its main objective, which is to regulate communications surveillance in Nigeria.

In a bid to provide a clear procedural guideline for communications surveillance, this chapter highlighted the different stages of surveillance. These are the authorisation, the execution and the post-surveillance stages and recommended detailed procedural guidelines for all these stages of surveillance. The categorisation of the stages of surveillance was necessary for the development and implementation of sound and fair procedural guidelines for Nigeria's communications surveillance regime. Provision was made for practical recommendations that were targeted at ensuring the

eradication of unlawful and arbitrary communications surveillance practices at every stage of surveillance.

These recommendations include limiting the use of communications surveillance to instances where there are no alternative means of achieving the purpose of the surveillance as well as the establishment of an OSI that will oversee the execution of communications surveillance rather than the LEOs. Another recommendation is prohibiting the access of LEOs to surveillance information that is not required for the investigation, thus eliminating undesirable disclosures. Furthermore, it is necessary to ensure that the Communications Surveillance Act makes provision for punitive measures for LEOs who falsify information in surveillance applications.

In terms of an independent and effective oversight mechanisms for communications surveillance in Nigeria, this chapter recommended a Surveillance Panel to replace the current practice where judges are the authorising body. The appointment of the members of the Surveillance Panel must be independent from the executive, and its members must be appointed by the Judicial Service Commission. This will enable independence of the authorising body from the State. It was recommended that members of the Surveillance Panel should consist of experts in ICT, surveillance and data privacy laws and they should have the sole duty of authorisation and supervision of the surveillance procedure. This proposal seeks to promote the effectiveness of the authorising body by ensuring that there is adequate expertise to handle surveillance matters.

With regard to an effective avenue for redress, it was recommended that post-surveillance notification is a germane factor to achieving redress. An automatic review of every stage of the surveillance procedure was also suggested in order to ensure that all surveillance subjects are provided with an opportunity to achieve redress irrespective of their financial capacity. Lastly, the development of a tort of the infringement of the right to privacy is needed, as this will facilitate an effective means of providing for civil damages and the appropriate compensation of surveillance subjects.

The next chapter concludes the thesis by summarising the key research findings and answering the research questions posed in chapter one.

CHAPTER SIX

CONCLUSION

6.1 Introduction

This chapter answers the research questions posed in chapter one. The main question that this study addresses is how the Nigerian legislative framework on communications surveillance can be reformed to conform with international standards. Four sub-questions were formulated to enable an analysis of the issues that emanate from the main question. These sub-questions are posed below and answered. Thereafter, an answer is provided for the main research question.

6.2 Research question one – The importance of right to communications' privacy in the digital age

The first sub-question enquires about the importance of the right to communications' privacy in the digital age and the impact of unlawful and arbitrary laws on communications surveillance in a democracy.

The advancement of information and communications technology (ICT) has created new threats to the right to privacy, particularly communications privacy. Chapter one highlighted the impacts of ICT on modern communications and detailed how electronic communications technology has become a standard component of life. Innovations in ICT have also given rise to many modern technologies that have improved the efficiency and effectiveness of electronic communications surveillance. As a result, one can conclude that the risk of communications surveillance on digital communications networks has become higher than in the past and it is important that there is adequate protection for the right to privacy of persons utilising digital communications technology.

Chapters one and two showed that the right to privacy is not absolute and that there are international and regional law standards to which national legislation on the regulation of communications surveillance must adhere. The analysis of case law of the European Court of Human Rights (ECtHR) leads to the conclusion that unlawful and arbitrary laws on communications surveillance can erode democracy. Moreover, such laws are often utilised to oppress and intimidate opponents, rather than for achieving the legitimate aims of surveillance, as recognised by international law.

6.3 Research question two – International and regional law standards on the regulation of communications surveillance

The second research question seeks to investigate the existing international, regional and sub-regional standards for legislation on communications surveillance. In answering this question, the study in chapter two explored these standards on the right to privacy and communications surveillance.

The findings in chapter two indicated that international and regional laws require that the execution of communications surveillance be backed by a legal framework that aligns with international law. The International Covenant on Civil and Political Rights (ICCPR) together with other United Nations (UN) documents address the international law standard on the limitation of the right to privacy. These UN documents are the 1988 UN Human Rights Committee CCPR General Comment No. 16 on article 17 (General Comment 16), the 2014 and 2018 reports of the Office of the High Commissioner of Human Rights (OHCHR), the Siracusa Principles on the limitation and derogation provisions in the ICCPR and the UN Special Rapporteurs report on human rights and fundamental freedoms while countering terrorism (SR report on counterterrorism).

The ICCPR requires that laws limiting the right to privacy be lawful and non-arbitrary. The terms “lawful and non-arbitrary” mean that the limitation must be reasonable (necessary and proportionate to the end sought) and pursue a legitimate aim. Domestic legislation regulating communications surveillance must reflect the broad guidelines on limiting the right to privacy as provided by international law. In particular, the SR report on counterterrorism provides a four-part proportionality test for evaluating whether a limitation of the right to privacy is arbitrary.¹⁴⁰⁸ This test evaluates whether: a legitimate aim is pursued; the legitimate aim is rationally connected to the measure taken to limit the right to privacy; the impairment is minimal; and; there is a fair balance struck between the legitimate aim pursued and the right to privacy.

¹⁴⁰⁸ Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, OHCHR, A/HRC/13/37 pars [14-19], (28 December 2009) (Martin Scheinin) [SR report on counterterrorism]; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OHCHR, U.N. Doc. A/HRC/23/40 (17 April 2013) (by Frank La Rue), [hereinafter Special Rapporteur 2013 Report] pars [28-29]; Novak *U.N. Covenant on Civil and Political Rights: CCPR Commentary* 2ed (2005), 378.

African regional law, specifically the Declaration on Freedom of Expression and Access to Information, 2019 (the 2019 Declaration), mandates the Member States of the African Union (AU) to comply with international law guidelines on the regulation of communications surveillance. Nigeria and South Africa as Member States of the AU are required to ensure that their domestic courts undertake a proportionality analysis when adjudicating on cases relating to the limitation of rights. Although most of the guidelines for regulating communications surveillance provided in the 2019 Declaration are generally broad and similar to international law guidelines, some of them provide specific guidance. These include providing that the judiciary must be the pre-authorisation body for a communications surveillance order and the need for a mandatory post-surveillance notification.

Some of the provisions in the 2019 Declaration, however, do not provide optimal protection for human rights during surveillance. For example, a judge presiding over an application of a communications surveillance order may be independent but could lack the ICT expertise required to understand the technicalities involved in the execution of a communications surveillance order. The judge may also not understand the dynamics of digital privacy and how intrusive privacy communications surveillance has become. The result is that a communications surveillance order could be evaluated along the same lines as a regular warrant. Whereas a communications surveillance order is effective only when the surveillance subject is ignorant, the defendant of a regular warrant is eventually notified when the order is executed and can challenge the process.¹⁴⁰⁹ This means that surveillance subjects are unable to defend themselves and provide the judge with relevant information that will ensure that their rights are adequately protected. The effective regulation of communications surveillance therefore requires both legal and ICT expertise that may be best suited for a non-judicial panel.

Having explored international and African regional law, it became apparent that neither the Human Rights Committee (HRC) nor the African Court of Human Rights (ACtHR) has presided on any cases relating to communications surveillance where they could apply these guidelines. As a result, the study examined European regional law and used the judgments of the European Court on Human Rights (ECtHR), which has

¹⁴⁰⁹ *AmaBhungane v Minister of Justice* 2021 (4) BCLR 349 (CC) par [84].

presided over several cases on communications surveillance and is the leading authority globally on the regulation of communications surveillance.

The ECtHR applies both international and European regional law to the domestic laws that are being scrutinised. The judgments of the ECtHR on communications surveillance therefore provide excellent guidance for Nigeria as it applies international law to these cases. The decisions of the ECtHR that were relevant to this study include those of *Weber and Saravia v Germany*, *Zakharov v Russia*, *Bigbrother Watch v United Kingdom* and *Kennedy v United Kingdom* as they reflected clear examples of communications surveillance practices to emulate or avoid.¹⁴¹⁰ The ECtHR in their adjudication of these cases has provided minimum safeguards that domestic laws regulating communications surveillance must stipulate. These minimum safeguards are similar to international law guidelines on communications surveillance and have been used in this study to recommend reforms for the legal framework of communications surveillance in Nigeria.

Chapter two concluded that the international and regional guidelines for communications surveillance require that laws regulating communications surveillance must be clear, comprehensive, precise and foreseeable; they must furthermore provide for effective procedural guidelines and independent authorisation and supervisory bodies. In the final instance, they must provide for adequate avenues for the surveillance subject to seek redress.

6.4 Research question three – The lessons for Nigeria from the South African legal framework on communications surveillance

The third research question examines whether South Africa's communications surveillance regime is lawful and non-arbitrary and how Nigeria can learn from South Africa's jurisprudence on the right to privacy and its communications surveillance regime.

This investigation was conducted in chapter three and it explored how communications surveillance is regulated in South Africa. It revealed sound jurisprudence on the protection of privacy. South Africa's communications surveillance regime is

¹⁴¹⁰ *Weber and Saravia v Germany* par App. no. 54934/00, 2006-XI Eur.Ct.H.R.; *Zakharov v Russia*, App. No. 47143/06, (2015); *Kennedy v United Kingdom*, App. no. 26839/05 (18 May 2010); *Bigbrother Watch v UK* App. nos. 58170/13, 62322/14, 24960/15 (2018).

spearheaded by the Constitution (which protects the right to privacy) with RICA¹⁴¹¹ as the primary law regulating communications surveillance. The South African law on the protection of the right to privacy provides a good foundation for testing laws that restrict human rights. This is evidenced by the decisions of the High Court and Constitutional Court in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* where some sections of the RICA were declared unconstitutional.¹⁴¹²

The Constitutional Court declared sections 1, 16, 35 and 37 of the RICA unconstitutional.¹⁴¹³ Section 16 was challenged because of its prohibition of post-surveillance notification and the inadequate safeguard for the right to a fair hearing resulting from the *ex parte* nature of surveillance applications.¹⁴¹⁴ On this challenge, the Constitutional Court held that post-surveillance notification of the surveillance subject should be the default position. Post-surveillance notification provides the surveillance subject an opportunity to review the communications surveillance order.¹⁴¹⁵

In addition, sections 1 and 16 provide for the mode of appointment and duties of the designated judge respectively but fail to ensure judicial independence. Sections 35 and 37 of the RICA were declared unconstitutional because they fail to provide adequate safeguards for the post-surveillance processing of information acquired from communications surveillance.¹⁴¹⁶ The Constitutional Court declared that access to post-surveillance information must be limited to what is strictly necessary for an investigation.

To answer the first part of research question three: post the decision in *AmaBhungane*, the RICA now provides for a communications surveillance regime that is lawful and non-arbitrary and is a good example of a legal framework for Nigeria to emulate. There are many lessons for Nigeria that were discussed in detail in chapters three and five. To summarise, firstly, South African privacy jurisprudence has shown that a

¹⁴¹¹ The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

¹⁴¹² 2020 (1) SA 90 (GP); 2021 (4) BCLR 349 (CC).

¹⁴¹³ *AmaBhungane v Minister of Justice* (CC) par [95].

¹⁴¹⁴ S.16(7)(a) of 70 of 2002.

¹⁴¹⁵ *AmaBhungane v Minister of Justice* (CC) pars [39,40].

¹⁴¹⁶ *AmaBhungane v Minister of Justice* (CC) par [108].

communications surveillance regime that is lawful and non-arbitrary is dependent on solid constitutional protection for the right to privacy with clear permissible restrictions. Using the South African jurisprudence and international law, recommendations were made for the way in which section 45 of the 1999 Constitution of the Federal Republic of Nigeria should be interpreted. In particular, the Nigerian courts should ensure that the laws limiting the right to privacy are evaluated based on whether they are reasonably justifiable in a democratic society.

Section 36(1)(a)-(e) of the South African Constitution provides factors that guide the South African courts when assessing the constitutional validity of statutes. These factors are an evaluation of the nature of the right, the importance of the purpose of the limitation, the nature and extent of the limitation, the relation between the limitation and its purpose and less restrictive means to achieve the purpose. These factors are similar to the four-part proportionality test provided in the SR report on counterterrorism. Chapter five of this thesis recommended that the four-part proportionality test and the factors provided for in section 36(1)(a)-(e) of the South African Constitution be used as an example for the Nigerian courts when evaluating whether a limitation of a right is reasonably justifiable.

Secondly, the RICA provides detailed procedural guidelines for the execution of communications surveillance. These guidelines informed some of the recommendations for the reforms proposed for Nigeria in chapter five. Specifically, the RICA provides that a designated judge must have full access to all information regarding the surveillance application. This provision is pivotal to the effective performance of the designated judge's duty as the law enforcement officer (LEO) is obliged to present all material facts pertaining to the application. The designated judge will therefore be able to deliver a well-reasoned decision for the grant or rejection of the surveillance application.

Thirdly, the South African communications surveillance regime requires that information that is not relevant to the investigation must be destroyed in order to prevent undesirable disclosures. This happened in *AmaBhungane* to restrict the accessibility of surveillance information only to those persons who strictly need the information for the investigation. This is a unique provision that is recommended for Nigeria.

Fourthly, using South Africa as a comparator, the thesis concludes that it is necessary for Nigerian courts to develop a tort of invasion of privacy. For an invasion of privacy to be actionable under the common law of tort there must be a reasonable expectation of privacy, the invasion must be intentional and wrongful. The development of a tort of privacy will enable a prejudiced party to claim compensation in tort against the State in addition to a declaration of right. This will enable the courts to have a principle in civil law that can be balanced with constitutional provisions to provide adequate compensation to the victim of an unlawful surveillance.

6.5 Research question four – The need for a comprehensive statute regulating communications surveillance in Nigeria

The fourth research question deals with the legal reforms that are necessary to ensure a communications surveillance regime that adequately protects the right to privacy in Nigeria. Chapter four of the thesis identified the problems with the communications surveillance regime in Nigeria. The first problem discussed was the incorrect interpretation of section 45 of the 1999 Nigerian Constitution by the courts. It was shown that most courts favour laws permitting governmental actions that limit the right to privacy without conducting an evaluation to determine whether the law is reasonably justifiable as provided by section 45.

The Nigerian courts need to interpret section 45 in light of international law, which defines the term “reasonable” as a limitation that is necessary and proportional to the end sought. This evaluation is summed up in the four-part proportionality test that is recommended in the SR report on counterterrorism and exemplified by section 36(1) of the Constitution. The decision in *AmaBhungane* demonstrates how the factors for determining whether a law is reasonable and justifiable in section 36(1) can be applied practically to the limitation of the right to privacy. These factors assisted the Constitutional Court in analysing the RICA and in declaring the contested provisions unconstitutional. Chapter five recommends that the Nigerian courts emulate the South African approach to limitation of rights adjudication as it reflects international law standard.

Another problem in Nigeria is the absence of a comprehensive statute on communications surveillance in Nigeria, an issue which needs to be addressed by the legislature. The research demonstrated that a statute that is clear, precise and

foreseeable must be enacted. The concept of foreseeability in this context means that there must be sufficient detail about the nature of offences that can prompt surveillance. It also refers to the clarity of the law in respect of the circumstances under which a person becomes a subject of surveillance, that is, whether the person is suspected of, accused of, or possesses information about a defined offence. The statute must further provide clarity on the authorised persons to conduct surveillance and the statute must ensure that communications surveillance be preauthorised by the appropriate authorisation body. Ultimately, the statute must focus on protecting the right to privacy rather than merely enabling communications surveillance.

An effective procedural framework at all stages of communications surveillance is also required. A competent authorisation body is needed with supervisory functions for the procedure. Also, the current surveillance structure in which law enforcement officers implement the surveillance order must be replaced by an independent institution that is constituted by competent persons who are ICT experts and/or data privacy law experts. These persons will also have the duty to separate relevant from non-relevant information, discarding the latter. In this way, the risk of occurrence of undesirable disclosures of the information of the surveillance subject will be diminished. This procedure ensures the protection of the privacy of the surveillance subject at both implementation and post-surveillance stages.

An independent oversight body is also an integral part of a surveillance regime that provides adequate protection for human rights. Chapter five explored the best options for Nigeria in this respect by comparing a judicial (current approach) and non-judicial panel approach. The non-judicial panel approach was recommended as the best suited for Nigeria as a panel increases the possibility of presiding officers having a broad perspective. This is necessary because the inability of the surveillance subjects to defend themselves may inhibit a fair hearing. The non-judicial panel should also have an expert on the panel, thus providing for a more diverse range deliberations on the issues to be adjudicated. The South African and German surveillance regimes, discussed in chapters two, three and five, provide valuable guidance in respect of a panel of experts as the oversight body for communications surveillance.

Although a comparative study between Germany and Nigeria was not undertaken in this research, the decision of the ECtHR in *Weber and Saravia v Germany* in which the German communications surveillance regime was declared as compliant with the

ECHR and international law, could not be ignored. The study took advantage of some of Germany's procedural rules that are notable and recommended them for Nigeria. These rules are the establishment of a non-judicial independent panel as the authorising body and the provision of both civil and constitutional remedies to an aggrieved surveillance subject to seek redress.

Furthermore, there must be an effective avenue for redress that is readily available and accessible to all surveillance subject irrespective of financial status. Post-surveillance notification is an important recommendation in this regard as it may otherwise be impossible for the surveillance subject to be aware of the surveillance. Provision should be made for an automatic review at no cost that will enable persons who are financially incapable to seek redress for any unlawful surveillance. It was also argued that constitutional damages is inadequate to provide compensation to the victim of an unlawful surveillance. A civil remedy through a tort of privacy should be introduced. The South African model, discussed in chapter three, that permits common law damages in addition to constitutional relief for an infringement of a right to privacy is recommended.¹⁴¹⁷

6.6 Research question five – The recommendations for the reform of the legal framework of communications surveillance in Nigeria

Having highlighted the problems with the current Nigerian legal framework on communications surveillance, there are concrete steps that must be followed for the reforms to be actualised, which encapsulates research question five. Firstly, a comprehensive statute that focuses on the regulation of communications surveillance is needed. The title of the statute must reflect its purpose. A suggested name is “The Regulation of Electronic Communications Surveillance Act” (Surveillance Act). The Surveillance Act must be the primary law on communications surveillance in Nigeria and repeal the Lawful Interception of Communications Regulation (LICR), 2019. It

¹⁴¹⁷ Chapter 3, sec.3.6.4; Section 8(2) of the Constitution; Ss. 39(2) and (3) of the Constitution; *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg v Minister of Police* 2022 (1) BCLR 46 (CC) pars [91-103]; *Komape v Minister of Basic Education* 2020 (2) SA 347 (SCA) par [41]; *Khumalo v Holomisa* 2002 (5) SA 401 (CC) pars [30-31, 33]; *Ngomane v Johannesburg (City)* 2020 (1) SA 52 (SCA) pars [22-27]; *Fose v Minister of Safety and Security* 1997 (7) BCLR 851 (CC) par [67]; *Veldman v Director of Public Prosecution, Witwatersrand Local Division* 2007 (3) SA 210 (CC) par [26]; Currie and De Waal *The Bill of Rights Handbook* 6ed (2013) 46; Van der Walt and Midgley (eds) *Principles of Delict* 4ed (2016) 7.

must also amend sections 9, 38, 39, 45(2)(a) and(f), 50 of the Cybercrimes (Prohibition, Prevention etc) Act, 2015 and section 29 of the Terrorism (Prevention and Prohibition) Act, 2022 (TPPA) to refer to the new statute on matters relating to communications surveillance.

The Surveillance Act must further provide that the law-making power in section 70(1) of the Nigerian Communications Act, 2003 (NCA) excludes the regulation of communications surveillance. This is because section 70(1) is currently interpreted as empowering the NCC to formulate laws that regulate communications surveillance which led to the formulation of the LICR. The discussion in chapter four shows that communications surveillance is utilised by law enforcement agencies (LEAs). Formulating laws that regulate communications surveillance amounts to regulating the activities of LEAs. The legislature is the only organ of government that is constitutionally empowered to enact laws on matters relating to law enforcement. This means that the LICR is an overreach of the powers of the NCC that must be rectified by a clear provision in the Surveillance Act repealing the LICR.

Secondly, the Surveillance Act must state clearly and precisely that communications surveillance in Nigeria is unlawful unless it is executed in terms of the Act. The following details must be specified: the authorised persons to execute surveillance; the legitimate purposes for which surveillance can be executed, the procedures for the execution of surveillance; the duration of the surveillance period and the circumstances in which a person can be subjected to surveillance. Chapter five furthermore recommends that the approach in the RICA be adopted in Nigeria, with chapter one of the Surveillance Act specifying the law enforcement agencies and the designation of officers that can be qualified to apply for the execution of communications surveillance.

Only these law enforcement agencies will be qualified to apply for a communications surveillance order. In Nigeria the qualified agencies will be the Nigeria Police Force (criminal investigations), Nigerian Defence Force, National Intelligence Agency (foreign intelligence matters), State Security Services (domestic intelligence), Economic and Financial Crimes Commission (financial fraud), and the National Drug Law Enforcement Agency (NDLEA - dealing in drugs). To this end, the Surveillance Act must repeal sections 146 and 147 of the NCA that enables communications service providers (CSPs) to initiate communications surveillance unilaterally. The

RICA also ensures that the qualified officers may only request surveillance for matters relating to their areas of expertise. This will mean, for example, that only the NDLEA can apply for surveillance on matters relating to drugs dealing offences.

The communications surveillance order must be executed by an independent surveillance intermediary as per the German approach, discussed in Chapter five. The legitimate purposes for applying for surveillance must also align with section 45 of the 1999 Nigerian Constitution and where surveillance is required for criminal justice purposes, it can be applicable to serious crimes only. The crimes that qualify as serious crimes must also be specified in the new statute as reflected in the schedule to the RICA. These crimes include high treason, any offence relating to terrorism, any offence involving sabotage, sedition, any offence that could result in the loss of a person's life or serious risk of loss of life.¹⁴¹⁸ Other crimes that may be included are offences relating to: racketeering, criminal gang activities, dealing in drugs, dealing in or smuggling of ammunition, firearms, explosives or armament, any offence the punishment whereof may be imprisonment for life or a period of imprisonment exceeding five years without an option of fine. The gravity of the harm caused by these offences provides a ground for the limitation of the right to privacy that is as intrusive as communications surveillance.

Regarding the duration of the communications surveillance order, it is recommended that an order be valid for three months after which a new application must be made. This approach is in line with the South African and German laws on communications surveillance. In relation to the circumstances for which a person may be under surveillance, the Surveillance Act must state specifically that surveillance will be permitted if there is a reasonable suspicion that a serious crime has been, is being or is about to be committed. In addition, there must be a potential or actual threat to national security, public health, and public order and safety. Where surveillance relates to persons possessing information about a serious crime, there must be concrete evidence supporting the assertion and the particulars of information that is required from the person must be detailed in the application.

¹⁴¹⁸ Also, the offences referred to in articles 6, 7 and 8 of Rome Statute of the International Criminal Court.

Thirdly, the Surveillance Act must provide for a detailed procedure at all stages of the surveillance. The communications surveillance procedure proposed in chapter five requires the involvement of two bodies, namely the Surveillance Tribunal and the Office of the Surveillance Intermediary (OSI). The Surveillance Tribunal must be constituted by the Judicial Service Commission (JSC) with a non-renewable term of two years to ensure its independence. The JSC must also appoint the head of the OSI. The Surveillance Tribunal will be responsible for the authorisation, supervision and post-surveillance notification of communications surveillance. The OSI must conduct the execution and the post-surveillance processing of the surveillance information acquired.

The duties of the OSI also include developing the technical procedures for the execution of surveillance that will be approved by the Surveillance Tribunal. An application for a communications surveillance order must be made to the Surveillance Tribunal and, if successful, the order must be forwarded to the OSI for execution. The information acquired by the OSI will then be organised and only information relevant to the investigation will be submitted to the applicant. The applicant will notify the OSI once the information is no longer in use and the latter must store such information for three years after which it will be destroyed. The OSI will submit a report to the Surveillance Tribunal every six months, and this must include an application for automatic review of the executed surveillance. The latter must submit an annual report to the legislature.

Lastly, the Surveillance Act must provide for post-surveillance notification that will be issued by the Surveillance Tribunal to the surveillance subject with the automatic review report. This will be served by the Surveillance Tribunal when it has reached a decision that the investigation will not be jeopardised. The surveillance subject may then decide to challenge the surveillance procedure at the Federal High Court and seek compensation for unlawful communications surveillance.

6.7 Main research question

This study seeks to investigate how the Nigerian legislative framework on communications surveillance should be reformed to conform with the standards in international law. As has already been shown, to do so, the Nigerian legal framework on communications surveillance must be lawful and non-arbitrary. The main aim of

international law when addressing the regulation of communications surveillance is to ensure that the right to privacy and other rights of the surveillance subject are adequately protected. The three arms of government of Nigeria, that is the legislature, the judiciary and the executive, have important roles to play in the reformation of Nigeria's framework.

The legislature needs to be educated about the capacity of communications surveillance to erode democracy and the need to enact a statute that ensures the preservation of human rights. The legislature must also be aware of the international and regional law standards on the regulation of communications surveillance. The legislature is urged to consider the recommendations set out in this thesis for incorporation into a new statute. The judiciary should ensure that section 45 of the 1999 Constitution is correctly interpreted so as to prevent undue limitation of people's fundamental rights.

The proposed statute, that is the Surveillance Act must provide for clear, precise and comprehensive obligations for the executive when communications surveillance is required. The Surveillance Act must also ensure that the executive has limited discretionary powers in respect of communications surveillance. Ultimately, if reformation is to occur in a manner which best protects human rights and the Nigerian democracy, the recommendations for a communications surveillance regime in Nigeria as proposed in this study should be implemented.

6.8 Conclusion

This study has demonstrated that innovations in ICT have increased the capacity of the State to monitor electronic communications. Law must develop to align with the current global trends in this regard. The Nigerian legal framework is intrusive and does not adequately protect human rights, specifically the right to privacy. A legal framework for communications surveillance must provide adequate safeguards for the right to privacy and other rights affected by surveillance.

The reforms recommended in this thesis are designed to overcome the current problems in the Nigerian law and also provide an original and significant contribution to the development of the Nigerian law on communications surveillance. It is recommended that a new and comprehensive legislative regime be implemented in Nigeria to ensure that the right to privacy is protected adequately when

communications surveillance is being executed. Regulation in this form will also strengthen the Nigerian democracy and the human rights of the Nigerian people.

BIBLIOGRAPHY

TABLE OF INTERNATIONAL INSTRUMENTS

United Nations

UN Human Rights Committee *CCPR General Comment No. 16: Article 17. (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988.

Convention on the Rights of the Child 1577 UNTS 3. Adopted: 20.11.1989; EIF: 2.09.1990.

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families 2220 UNTS 3. Adopted: 18.12.1990; EIF: 1.07.2003.

International Covenant on Civil and Political Rights 999 UNTS 171. Adopted: 16.12.1966; EIF: 23.03.1976.

International Covenant on Economic, Social and Cultural Rights 993 UNTS 3. Adopted: 16.12.1966; EIF: 3.01.1976.

UN Commission on Human Rights *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (28 September 1984) E/CN.4/1985/4.

UN General Assembly *Universal Declaration of Human Rights* (10 December 1948) Resolution 217 A (III).

Vienna Convention Law of Treaties 1155 UNTS 331. Adopted: 23.05.1969; EIF: 27.01.1980.

African Union (AU)

African Charter of Human and Peoples' Rights 1520 UNTS 217. Adopted: 27.06.1981; EIF: 21.10.1986.

African Charter on the Rights and Welfare of the Child. Adopted: 11.07.1990. EIF: 29.11.1999.

African Commission on Human and Peoples' Rights *Declaration on Freedom of Expression and Access to Information*, adopted at the 65th Ordinary Session held 21 October to 10 November 2019, Banjul, The Gambia.

African Union Convention on Cyber Security and Personal Data Protection. Adopted: 27.06.2014; EIF: not yet.

Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights. Adopted: 06.10.1998; EIF: 25.06.2004.

Council of Europe (CoE)

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 Trans-border Data Flows 2001* (28 November 2001) ETS 181.

European Convention on Human Rights 213 UNTS 262. Adopted: 4.11.1950; EIF: 3.09.1953.

European Union (EU)

Charter of Fundamental Rights of the European Union

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters *OJL 350*, 30.12.2008 60-71.

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.

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).

Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

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 on the Free Movement of Such Data No L281/31 of 1995.

Economic Community of West African States (ECOWAS)

ECOWAS, Supplementary Act on Personal Data Protection within ECOWAS, Feb. 16, 2010, ECOWAS A/SA.JO1/10.

Southern African Development Community (SADC)

Protocol on the SADC Tribunal, 2001.

SADC Treaty, 1992

SADC Model Law on Data Protection, 2013

TABLE OF LEGISLATION

Germany

Restrictions on the Secrecy of the Mail, Post and Telecommunications Act of 13 August 1968 (Gesetz zur Beschränkung des Brief-, post under Fernmeldegeheimnisses, “the G 10” Act).

Nigeria

African Charter on Human and People’s Rights (Ratification and Enforcement) Act, Cap A9, LFN 2004.

Central Bank of Nigeria Act, No. 7 of 2007.

Child’s Right Act, 2003.

Constitution of the Federal Republic of Nigeria, 1999.

Consumer Code of Practice Regulation 2007, GN 56 in GG 87, Vol.94 of 2007-07-10.

Credit Reporting Act, 2017.

Criminal Code Act, Cap C38, LFN 2004.

Cybercrimes (Prohibition, Prevention, etc) Act, 2015.

Evidence Act, 2011.

Federal Competition and Consumer Protection Act, 2019.

Freedom of Information Act, 2011.

Fundamental Rights (Enforcement Procedure) Rules, 2009.

Interpretation Act Cap 123, LFN 2004

Lawful Interception of Communications Regulation, 2019.

Lagos State High Court (Civil Procedure) Rules 2019.

National Drug Law Enforcement Agency Act Cap. N30, LFN 2004.

National Health Act, 2014.

National Identity Management Commission Act, 2007.

National Information Technology Development Act, 2007.

National Security Agencies Act, 1986.

Nigerian Communications (Enforcement Process, etc.) Regulations, 2019.

Nigerian Communications Act, 2003.

Nigerian Communications Commission (Registration of Telephone Subscriber Regulation) 2011, GN101 in GG 229, Vol. 98 of 2011-11-07.

Nigerian Data Protection Regulation, 2019.

Nigerian Data Protection Regulation.

Nigerian Defence Act 1984.

Nigerian Police (Establishment) Act, 2020.

Public Order Act Cap 328, Laws of Federation of Nigeria 1990.

Same Sex Prohibition Act, 2013.

Terrorism (Prevention and Prohibition) Act, 2022.

The Child's Rights Act, 2003

The Consumer Code of Practice Regulation, GN 56 in GG 87, Vol.94 of 2007-07-10.

The Credit Reporting Act, 2017.

The Federal Competition and Consumer Protection Act, 2019.

The HIV and AIDS (Anti-Discrimination) Act, 2014.

The National Identity Management Commission Act, 2007.

The Registration of Telephone Subscribers Regulations, 2011, GN101 in GG 229, Vol. 98 of 2011-11-07.

Trade Unions Act 1986.

Russia

Russian State Secret Act of Law no. 5485-I, 21 July 1993.

Operational-Search Activities Act of 12 August 1995 (no.144-FZ).

Russian Code of Criminal Procedure of 18 December 2001 (CCrP).

Regulation no. 63 of 6 February 2010 of the government of the Russian Federation.

South Africa

Constitution of the Republic of South Africa, 1996.

Correctional Services Act 111 of 1998.

Criminal Procedure Act 51 of 1977.

Cybercrimes Act 19 of 2020.

Drugs and Drug Trafficking Act 140 of 1992.

Electronic Communications and Transactions Act 25 of 2002.

Extension of Security of Tenure Act 62 of 1997.

Intelligence Services Oversight Act 40 of 1994.

Interim Constitution of the Republic of South Africa Act 200 of 1993.

Judge's Remuneration and Conditions of Employment Act 47 of 2001.

Medicines and Related Substances Control Act 101 of 1965.

National Strategic Intelligence Act 39 of 1994.

Protection of Personal Information Act 4 of 2013.

Regulation of Interception and Provision of Communication-related Information Act 70 of 2002.

United Kingdom

Investigatory Powers Act, 2016.

United States of America

United States' Wiretap Act 18 United States Congress § 2510(4) (2000).

The United States Electronic Communications Privacy Act, 1986.

TABLE OF CASES

DECISIONS OF INTERNATIONAL BODIES

Human Rights Committee

Hulst v Netherland, Communication No. U.N.Doc. CCPR/C/82/D/903/1999 (2004).

Keun-Tae v Republic of Korea, Communication No.574/1994, CCPR/C/64/D/574/1994.

Toonen v Australia Communication No. U.N.Doc. CCPR/C/50/D/488/1992 (1994).

Velichkin v Belarus Communication No. 1022/2001, U.N Doc. CCPR/C/85/D/1022/2001.

Irina Fedotova v Russian Federation, Communication No. 1932/2010 (2012).

African Court of Human and Peoples Rights

Abubakari v Tanzania No. 007/2013 (2016).

Konaté v Burkina Faso, App. No. 004/2013 (2014).

African Commission of Human and Peoples Rights

African Commission on Human and Peoples Rights v Libya No. 002/2013 (2016).

Chacha v Tanzania No. 003/2012 (2014)

SADC

Chimexpan v Tanzania Case No. SADC (T) 01/2009 (2010).

Mike Campbell v The Republic of Zimbabwe SADC (T) Case No. 2/2007.

Council of Europe

Amann v Switzerland, App. No.27798/95, (2000).

Al-Nashif v Bulgaria, App. No. 50963/99 (2002).

Association for European Integration and Human Rights and Ekimdzhev v Bulgaria, App. No. 62540/00 (2007).

Bugallo v Spain, App. no. 58496/00 (2003).

Bigbrother Watch v UK, App. Nos. 58170/13, 62322/14 and 24960/15, Judgment on 13 September (2018).

Camenzind v Switzerland, App. No. 21353/93 (1997).

Centrum for Rattvisa v Sweden, App. No. 35252/08 (2019).

Chahal v United Kingdom, App. No. 22414/93 (1996).

Christie v United Kingdom, App. No. 21482/93 (1994).

Dumitru Popescu v Romania, (no. 2), App. No. 71525/01, (2007).

Hertzberg v Finland, Communication No. 61/1979 (1982).

Huvig v France, App. No. 11105/84 (1990) .

Iordachi v Moldova, App. No. 25198/02 (2009).

Kennedy v United Kingdom App. No. 26839/05 (2010).

Klass v Germany, App. No. 5029/71 (1978).

Konaté v Burkina Faso, App. No. 004/2013 (2014).

Kopp v Switzerland, App. No. 23224/94 (1998).

Kruslin v France, App. No. 11801/85 (1990).

Lambert v France, App. No. 46043/14 (2015).

Leander v Sweden, App. No. 9248/81 (1987).

Liberty v United Kingdom, App. No. 58243/001 (2008).

Liu v Russia, App. No. 42086/05 (2007).

Malone v United Kingdom, App. No. 8691/79, (1984).

P.G and J.H v United Kingdom, App. No. 44787/98 (2001).

Rotaru v. Romania, App. No.28341/95, (2000).

S and Marper v United Kingdom, App. Nos. 30562/04 and 30566/04 (2008).

M. K. v France, App. No.19522/09, (2013).

Valenzuela Contreras v Spain, App. No. 58/1997/842/1048 (1998).

Weber and Saravia v Germany, App. No. 54934/00 (2006).

Zakharov v Russia App. No. 47143/06, (2015).

European Union

Digital Rights Ireland and Seitlinger, C-293/12 and C-594/12 (2014).

Digital Rights Ireland; Secretary of Home Department v Watson App. No. C-201/15 and C-698/15 (2018).

Google Spain v Google C-131/12 (2014).

Nowak v Data Protection Commissioner, App. No. C-434/16 (2017).

Pretty v United Kingdom, App. No. 2346/02, ECHR (Fourth Section) 35 EHRR (2002).

Privacy International v Secretary of State for Foreign and Commonwealth Affairs EU Official Journal, App. No. C22 22/1/18 29-30 (2017).

Schrems v Facebook Ireland Ltd App. No C-498/16 (2018).

India

Manohar v Union of India, Supreme Court of India, Writ Petition (Criminal) No. 314 of 2021, 27 October 2021.

Nigeria

Abacha v Fawehimi (2000) 6 NWLR (Pt. 660).

Abdulkarim v Incar (Nig) Ltd (1992) NWLR (Pt. 251).

Aderinto v Omojola 1998(1) FHCLR.

Adigun v A.G Oyo State (No. 2) 1987 2 NWLR (Pt. 56).

Agbai v Okagbue (1991) 7 NWLR (Pt. 204).

Akuma Industries v Ayman Enterprises Ltd (1999) LPELR-13412 (CA).

Alamieyeseigha v FRN (2006) 16 NWLR Pt. 1004.

Ale v Obasanjo (1996) 6 NWLR (Pt. 459).

Anene v Airtel Nigeria Ltd, Suit No: FCT/HC/CV/545/2015 (unreported).

Aniekwe v Okereke (1996) 6 NWLR (Pt. 452).

Anigboro v Sea Trucks Ltd (1995) 6 NWLR (Pt. 399).

Anzaku v Governor of Nassarawa State (2006) All FWLR (Pt. 303).

Aqua Ltd v Ondo State Sports Council (1988) 4 NWLR (Pt.91) 622.

Aqua v Archibong (2012) LPELR-9293 (CA) 39.

Asari-Dokubo v Federal Government of Nigeria (2007) 12 NWLR (Pt. 1048).

Attorney General Bendel State v Attorney General of the Federation (1981) 10 SC

Attorney General of Abia State v Attorney General of the Federation (2002) 6 NWLR (Pt. 763).

Attorney General of Ogun State v Attorney General of the Federation (2003) FWLR (Pt.143).

Attorney General of Ondo State v Attorney General of the Federation (2002) 9 WLR (Pt.772).

Awolowo v Shagari (1979) 69 SC.

Bronik Motors Ltd v Wema Bank Ltd (1983) 1 SCNLR.

Chukwudi v Attorney General of the Federation (2010) LPELR-9047 (CA).

Chukwuma v Commissioner of Police (2005) 8 NWLR (Pt.927) 287.

Commissioner of Police, Ondo State v Obolo (1989) 5 NWLR (Pt. 1195) 130, 138.

Deduwa v Okorodudu (1974) 1 All NLR (Pt.1) 272.

Director of State Security Services v Agbakoba (1999) 3 SCNJ.

Duduruku v Nwoke (2015) 15 NWLR (Pt. 1483) 417, 474.

Edet Akpan v The State (1986) 3 NWLR (Pt.27) 25.

Emerging Markets Telecommunications Services Limited v Eneye (2018) LPELR-46193 (CA).

Enanuga v Sampson (2012) LPELR-8487 (CA).

Eneye v MTN Nigeria Communications Ltd, Appeal No: CA/A/689/2013 (unreported).

Fawehimi v Inspector General of Police (2002) LPELR 1258 SC.

Federal Republic of Nigeria v Daniel (2011) LPELR-4152 (CA).

Hassan v Economic and Financial Crimes Commission (2013) LPELR-22595 (CA).

Ibironke v MTN Nigeria Communications Ltd (2019) LPELR-47483 (CA).

Ifegwu v Federal Republic of Nigeria (2001) 13 NWLR (Pt. 229).

Igbokwe v Commissioner of Police Edo State (2017) LPELR-42072 (CA).

Igwe v Ezeanochie (2009) LPELR-11885 (CA).

Ikine v Edjerode (2001) 18 NWLR (Pt. 725).

Inspector General of Police v All Nigerian Peoples Party (2007) LPELR-8217 (CA).

Kim v State (1992) LPELR-1691 (SC).

Kotoye v Central Bank of Nigeria (1989) LPELR-1707 (SC).

Madume v Okwara (2013) LPELR-20752 (SC).

Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo (2001) LPELR-1856 (SC).

Minister of Home Affairs v Fisher (1972) 2 WLR (Pt.899).

Mitin v Commissioner of Police, Bayelsa State (2017) 43064 (CA).

Mojekwu v Mojekwu (1997) 7 NWLR 283 (C.A).

Muojekwu v Ejikeme (2000) 5 NWLR 402 (CA).

Nigerian Port Authority v Akar 1965 (1) All NLR.

Nosiru Attah v The State (1993) LPELR-598(SC).

Nwali v Ebonyi State Independent Electoral Commission (2014) LPELR-23682 (CA).

Nwankwo v The State [1985] 6 NCLR 228.

Nwanna v A.G of Federation (2010) LPELR-9047 (CA) 7.

Obadara v President Ibadan West District Council Grade B Customary Court 1964 1 All NLR.

Oceanic Securities International Ltd v Balogun (2013) All FWLR (pt. 667).

Ogbonna v Ogbonna (2014) 23 WRN 48.

Okafor v Ntoka (2017) LPELR-442794 (CA).

Okeke v Iheazie (2018) LPELR-45017 (CA).

Okoi v Inah 1998 (1) FHCLR.

Okonkwo v Ogbogu (1996) 5 NWLR (Pt.499).

Olafisoye v Federal Republic of Nigeria (2004) 4 NWLR (Pt. 804).

Olawoyin v Attorney General of Northern Nigeria (1961) ANLR 269.

Omonyahuy v The Inspector-General of Police (2015) LPELR-25581 (CA).

Onah v Okenwa (2010) 8 NWLR (Pt. 1195) 512, 536.

Onwo v Oko (1996) 6 NWLR (Pt. 456).

Osawe v Registrar of Trade Unions (1962) NWLR (Pt. 927).

Osha v Phillips (1972) 4 SC.

Oteri v Okoro Audu (1970) 1 All NLR 199.

Owena v Nigerian Stock Exchange Ltd (1997) 8 NWLR Pt. 515.

Ozide v Ewuzie (2015) LPELR-24482 (CA).

Rabiu v Kano State (1960) 8 SC.

Safiyatu v Attorney-General of Sokoto State (unreported judgement of the Sokoto State Shari'a Court of Appeal dated 25 March 2002).

Salubi v Nwariaku (1997) 5 NWLR (Pt. 505).

Sambo v Ndatse (2013) LPELR-20857 (CA).

Shugaba Darman v Minister of International Affairs (1980) FNL 203.

Solarin v Inspector General of Police (1983) 1 FNLR 415.

Tolani v Kwara State Judicial Service Commission (2009) LPELR- 8375 (CA).

Udo v Robson (2018) LPELR-45183 (CA).

Umeh v Kris Lorge Inu Ltd unreported case Suit No. CA/K/242/1996, 14 March 2001.

United Bank for Africa v Unisales (2014) LPELR-24283 (CA).

United Bank of Africa PLC v Ajabule (2012) 7 WRN 19.

Usman v The Executive Chairman, EFCC (2018) LPELR-44678 (CA).

Uzoukwu v Ezeonu II (1996) 6 NWLR (Pt. 200).

Williams v Majekodunmi (1962) 1 All Nigerian Law Report.

South Africa

AB and CB v Pridwin Preparatory School 2020 (5) SA 327 (CC).

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services 2021 (4) BCLR 349 (CC).

AmaBhungane v Minister of Justice and Correctional Services 2020 (1) SA 90 (GP).

Amod v Multilateral Motor Vehicle Accidents Fund (Commission for Gender Equality Intervening) 1999 (4) SA 1319 (SCA).

Azanian Peoples Organization (AZAPO) v President of the Republic of South Africa 1996 (4) SA 671 (CC).

Barkhuizen v Napier 2007 (5) SA 323 (CC).

Beadica v Trustees for the Time Being of the Oregon Trust 2020 (9) BCLR 1098 (CC).

Bernstein v Bester 1996 (2) SA 751 (CC).

Bosasa Operations (Pty) Ltd v Basson 2013 (2) SA 570 (GSJ).

Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Tourism 2004 (7) BCLR 687 (CC).

Case v Minister of Safety and Security; Curtis v Minister of Safety and Security 1996 (1) SACR 587 (CC).

Carmichele v Minister of Safety and Security 2001 (4) SA 938 (CC).

Cape Town Municipality v Bakkerud 2000 (3) SA 1049 (SCA).

Cape Town City v South African National Roads Authority 2015 (3) SA 386 (SCA).

Centre for Child v Media 24 Ltd 2020 (1) SACR.

Christian Education SA v Minister of Education 2000 (10) BCLR 1051 (CC).

Country Cloud Trading CC v MEC, Department of Infrastructure Development, Gauteng 2015 (1) SA 1 (CC).

Darson Construction (Pty) Ltd v City of Cape Town 2007 (4) SA 488 (C).

Dawood v Minister of Home Affairs; Shalabi v Minister of Home Affairs 2000 (8) BCLR 837 (CC).

DE v RH 2015 (5) SA 83 (CC).

De Klerk v Minister of Police 2020 (1) SACR 1 (CC).

De Lange v Smuts NO 1998 (3) SA 785 (CC).

Director-General, Department of Home Affairs v Link 2020 (2) SA 192 (WCC).

Director of Public Prosecutor, Transvaal v Minister of Justice and Constitutional Development 2009 (7) BCLR 637 (CC).

Director of Public Prosecution, Western Cape v Prins 2012 (2) SACR 183 (SCA).

Du Plessis v De Klerk 1996 (3) SA 850 (CC).

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

Economic Freedom Fighters v Speaker, National Assembly 2016 (3) SA 580 (CC).

Entabeni Hospital Ltd v Van der Linde/ First National Bank of SA v Puckriah 1994 (2) SA 422 (N).

Estate Agency Affairs v Auction Alliance (Pty) Ltd 2014 (3) SA 106 (CC).

Everfresh Market Virginia (Pty) Ltd v Shoprite Checkers (Pty) Ltd 2012 (1) SA 256 (CC).

F v Minister of Safety and Security 2012 (1) SA 536 (CC).

Ferreira v Levin; Vryenhoek v Powell 1996 (1) SA 984 (CC).

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

Fose v Minister of Safety and Security 1997 (3) SA 786 (CC).

Gardner v Whitwaker 1994 (5) BCLR 19 (E).

Gartner v Minister of Finance 2014 (1) BCLR 38 (CC).

Glenister v President of the Republic of South Africa 2009 (1) SA 671 (CC) (Glenister I).

Glenister v President of the Republic of South Africa 2014 (4) BCLR 481 (WCC) (Glenister II).

Gosschalk v Rossouw 1966 (2) SA 476 (C).

Gründling v Phumela Gaming and Leisure Ltd 2005 (6) SA 502 (SCA).

H v Fetal Assessment Centre 2015 (2) SA 193 (CC).

Helen Suzman Foundation v President of the Republic of South Africa; Glenister v President of the Republic of South Africa 2014 (4) BCLR 481 (WCC).

Hoffmann v SA Airways 2001 (1) SA 1 (CC).

Independent Institute of Education (Pty) Limited v Kwazulu-Natal Law Society 2020 (4) BCLR 495 (CC).

Independent Newspaper (Pty) Ltd v Minister for Intelligence Services: In re Masetlha v President of the Republic of South Africa 2008 (5) SA 31 (CC).

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit 2001 (1) SA 545 (CC).

Islamic Unity Convention v Independent Broadcasting Authority 2002 (4) SA 294 (CC).

Justice Alliance of South Africa v President of Republic of South Africa; Centre for Applied Legal Studies v President of Republic of South Africa 2011 (5) SA 388 (CC).

Kent v South African Railways 1946 AD 405.

Khumalo v Holomisa 2002 (5) SA 401 (CC).

Komape v Minister of Basic Education 2020 (2) SA 347 (SCA).

Law Society of South Africa v Minister for Transport 2011 (1) SA 400 (CC).

Le Roux v Dey (Freedom of Expression Institute and Restorative Justice Centre as Amici Curiae) 2011 3 SA 274 (CC).

Lee v Minister for Correctional Services 2013 (2) SA 144 (CC).

Loureiro v iMvula Quality Protection (Pty) Ltd 2014 (3) SA 394 (CC).

Magajane v Chairperson, Northwest Gambling Board 2006 (5) SA 250 (CC).

Maharaj v Mandag Centre of Investigative Journalism NPC 2018 (1) SACR 253 (SCA).

Mankayi v AngloGold Ashanti Ltd 2011(6) BLLR 527 (CC).

Mashongwa v Passenger Rail Agency South Africa 2016 (3) SA 528 (CC).

MEC, Department of Welfare v Kate 2006 (4) SA 478 (SCA).

Moise v Greater Germiston Transitional Local Council: Minister of Justice and Constitutional Development Intervening (Women's Legal Centre as Amicus Curiae) 2001 (4) SA 491.

Minister of Justice and Constitutional Development v Prince 2019 (1) SACR 14 (CC).

Minister of Police v Kunjana 2016 (2) SACR 473 (CC).

Minister of Police v Mboweni 2014 (6) SA 256 (SCA).

Minister of Safety and Security v Van der Merwe 2011 (5) SA 61 (CC).

Minister of Safety and Security v Van Duivenboden 2002 (6) SA 431 (SCA).

Minister of Welfare and Population Development v Fitzpatrick 2000 (7) BCLR 713 (CC).

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC).

Motor Industry Fund Administrators (Pty) Ltd v Janit 1994 (3) SA 56 (W).

My Vote Counts NPC v Minister of Justice and Correctional Services 2018 (5) SA 380 (CC).

National Coalition of Gay and Lesbian Equality v Minister of Justice 1999 (1) SA 6 (CC).

National Education Health and Allied Workers Union v University of Cape Town 2003 (3) SA 1 (CC).

National Media Ltd v Jooste 1996 (3) All SA 262 (A).

Nel v Roux NO 1996 (4) BCLR 592 (CC).

Ngomane v Johannesburg (City) 2020 (1) SA 52 (SCA).

Ngqukumba v Minister of Safety and Security 2014 (5) SA 112 (CC).

NM v Smith 2007 (5) SA 250 (CC).

MEC, Department of Welfare v Kate 2006 (4) SA 478 (SCA).

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC).

O’Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) All SA 159 (C).

Olitzki Property Holdings v State Tender Board 2001 (3) SA 1247 (SCA).

Pharmaceutical Manufacturers Association of South Africa: In re Ex parte President of the Republic of South Africa 2000 (2) SA 674 (CC).

Phillips v Director of Public Prosecution (WLD) 2003 (4) BCLR 357 (CC).

President of the Republic of South Africa v Hugo 1997 (4) SA 1 (CC).

Prince v Minister of Justice 2017 (4) SA 299 (WCC).

Protea Technology v Wainer 1997 (9) BCLR 1225 (W) 1241.

Qwelane v South African Human Rights Commission 2020 (2) SA 124 (SCA).

Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg v Minister of Police 2022 (1) BCLR 46 (CC).

S v A 1971 (2) SA 293 (T).

S v Bhulwan: S v Gwadiso 1995 (12) BCLR 1579 (CC).

S v Jaipal 2005 (1) SACR 215 (CC).

S v Makwanyane 1995 (3) SA 391.

S v Manamela (Director-General of Justice Intervening) 2000 (5) BCLR 491 (CC).

S v Negal: S v Solberg 1997 (10) BCLR 1348 (CC).

Sasol Synthetics Fuels (Pty) Ltd v Lambert 2002 (2) SA 21 (SCA).

Shabalala v Metrorail 2008 (3) SA 142 (SCA).

South African Association of Personal Injury Lawyers v Heath 2001 (1) SA 883 (CC).

South African Broadcasting Corporation v Avusa Ltd 2010 (1) SA 280 (GSJ).

Steenkamp v Provincial Tender Board, Eastern Cape 2007 (3) SA 121 (CC).

Stopforth Swanepoel & Brewis Inc. v Royal Anthem (Pty) Ltd 2015 (2) SA 539 (CC).

Teddy Bear Clinic for Abused Children v Minister of Justice and Constitutional Development 2014 (1) SACR 327 (CC).

Telematrix (Pty) Ltd t/a Matrix Vehicle Tracking v Advertising Standards Authority 2006 (1) SA 461 (SCA).

Thint (Pty) Ltd v National Director of Public Prosecutions; Zuma v National Director of Public Prosecutions 2008 (12) BCLR 1197 (CC).

Tshabalala-Msimang v Mahkanya 2008 (6) SA 102 (W).

Thomas v Minister of Home Affairs 2000 (8) BCLR 837 (CC).

Twee Jonge Gezellen (Pty) Ltd v Land and Agriculture Development Bank of South Africa t/a the Land Bank 2011 (3) SA 1 (CC).

Van Eden v Minister of Safety and Security 2003 (1) SA 389 (SCA).

Veldman v Director of Public Prosecution, Witwatersrand Local Division 2007 (3) SA 210 (CC).

Zuma v National Director of Public Prosecutions 2008 (12) BCLR 1197 (CC).

United Kingdom

A v B PLC [2003] Q.B. 195.

Bernstein of Leigh v Skyviews and General Ltd [1978] QB 479.

Campbell v MGN (2004) UKHL 22.

Dumbell v Roberts (1964) 1 All E.R 326.

Hunter v Southam Inc. (1984) 11 DLR (4th) 641 (SCC).

Hussain v Choong Fook Kam (1969) 3 All E.R. 1926.

Imerman v Tchenguiz (2011) Fam 116.

Kaye v Robertson and Sport Newspapers Ltd [1991] FSR 62.

Khorasandjian v Bush [1993] QB.

McKinley Transport Ltd v The Queen (1990) 68 DLR (4th).

QB in R (Davis and Others) v Secretary of State for the Home Department [2015] EWHC 2092 (17/07/2005).

Re X [1984] 1 WLR 1422.

Sheldon v Broomfield (1964) 2 Q.B. 578.

Tolley v Fry [1931] AC 333.

Wright v Home Office [2003] United Kingdom House of Lords 53, 16 October 2003.

United States of America

Abel v United States 362 US 217 (1960).

Carpenter v United States, 22 June 2018, 585 U.S_ (2018).

Hunter v Southam Inc. (1984) 11 DLR (4th) 641 (SCC).

Katz v United States 389 US 347 (1967).

Myers v United States (1962).

Smith v Maryland, 442 U.S 735 (1979).

United States v Dionisio 420 US 1 (1975).

United States v Mara 410 US 19 (1973).

Olmstead v United States 277 US 438 (1928).

WB v H Bauer Publishing Ltd (2002) Entertainment and Media Law Reports 145.

BOOKS AND CHAPTERS IN BOOKS

Ahmed, D. and Bulmer, E. "Limitation Clauses" in *International IDEA (Institute for Democracy and Electoral Assistance) Constitution-Building 2ed* (2017) Stockholm: Sweden.

Albers, M. "Surveillance and Data Protection Rights: Data Retention and Access to Telecommunications Data – Brazilian and German Approaches" in Albers, M. and Sarlet, I.W. (eds) *Personality and Data Protection Rights on the Internet* (2022) Springer Nature: Switzerland.

Allmer, T. *Towards a Critical Theory of Surveillance in Informational Capitalism* (2012) Peter Lang: Frankfurt.

Bernal, P. *Internet Privacy Rights: Right to protect autonomy* (2014) Cambridge University Press: Cambridge.

Benhabib, S., Waldron, J., Honig, B. and Kymlicka, W. *Another Cosmopolitanism* (2006) Oxford University Press: USA.

Bouchard, C. "The United Nations in the Digital Age: Harnessing the Power of New Digital Information and Communication Technologies" in Bjola and Zaiotti (eds) *Digital Diplomacy and International Organisations: Autonomy, Legitimacy and Contestation* (2020) Routledge.

Brown, G. *A Report by the Global Citizenship Commission - The Universal Declaration of Human Rights in the 21st Century: A Living Document in a Changing World* (2016) Open Book Series: Netherlands.

Bygrave, L.A. *Data privacy law: An international perspective* (2014) Oxford University Press: Oxford.

Casse, A. *International Law* 3ed (2020) Oxford University Press: England.

Cohen-Eliya, M. and Porat, I. *Proportionality and Constitutional Culture (Cambridge Studies in Constitutional Law)* (2013) Cambridge University Press: England.

Cohen, E.D. "Mass Surveillance and State Control: The Total Information Awareness Project" (2015) Palmgrave Macmillan: USA.

Currie, I. and de Waal, J. *The Bill of Rights Handbook* 6ed (2013) Juta and Company Ltd: Cape Town.

Nguyen, Q.D., Daillier, P., Forteau, M., and Pellet, A. *Droit International Public* 8ed (2009) Montchrestein-Lextenso: Paris.

DeCew, J.W. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (1997) Cornell University Press: New York.

Dembour, M. and Kelly, T. (eds) *Are Human Rights for Migrants?: Critical Reflections on the Status of Irregular Migrants in Europe and the United States* (2012) Routledge: Abingdon.

De Schutter, O. *International Human Rights Law* 3ed (2019) Cambridge University Press: Cambridge.

De Stadler, E. and Esselaar, P. *A Guide to the Protection of Personal Information Act* (2015) Juta: Cape Town.

Diala, A. "The Dawn of Constitutionalism in Nigeria" in *Constitutionalism and democratic governance in Africa: Contemporary perspectives from sub-Saharan Africa* Mbondenyi, M. K and Ojienda, T (eds.) (2013) Pretoria University Law Press: Pretoria.

Duncan, J. *The Rise of the Securocrats: The Case of South Africa* (2014) Jacana Media: Johannesburg.

Duncan, J. *Stopping the Spies: Constricting and Resisting the Surveillance State in South Africa* (2018) Wits University Press: Johannesburg.

Eijkman, Q. "Indiscriminate Bulk Data Interception and Group Privacy: Do Human Rights Organisations Retaliate through Strategic Litigation?" in Taylor, Floridi and Van der Sloot (eds) *Group Privacy* (2017) Springer International Publishing: Switzerland.

Foucault, M. *Discipline and Punish: The Birth of the Prison* (1995) Vintage Books: New York.

Fitzmaurice, M. *History of Article 38 of the Statute of ICJ* in Besson and d'Aspremont (eds) *The Oxford Handbook of the Sources of International Law* (2017) Oxford University Press: Oxford.

Fabbrini, F. and Vermulen, M. "GPS Surveillance and Human Rights and the United States Supreme Court in Comparative Perspective" in Davis, McGarrity and Williams (eds) *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (2014) Routledge: London.

Feldman, M. *The Internet Revolution and the Geography of Innovation* UNESCO (2002) Blackwell Publishers: Oxford.

Geist, M. "Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era" *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (2015) University of Ottawa Press.

Glendon, M.A. *Whole Made New: Eleanor Roosevelt and the Universal Declaration of Human Rights* (2001) Random House: New York.

Gray, D. and Henderson, S. (eds.), *The Cambridge Handbook of Surveillance Law* (2017) Cambridge University Press: Cambridge, England.

Gutwirth, S. *Privacy and the Information Age* (2002), Rowman & Littlefield: Maryland

Halperin, T. D. *The Alien and Sedition Acts of 1798: Testing the Constitution* (2016) Hopkins University Press: Baltimore.

Harris, D. O'Boyle, M., Bates, E. and Buckley, C. *Laws of the European Convention on Human Rights* 4ed (2018) Oxford University Publishing: Oxford.

Hill, D. *Jean-Francois Lyotard and the inhumanity of internet surveillance* in Fuchs, C. Boersma, K. Albrechtslund, A. and Sandoval, M. (eds.) *Internet and surveillance: The Challenges of Web 2.0 and Social Media* (2011) Routledge: New York.

Hynes, M. "Online Privacy and Surveillance" in *The Social, Cultural and Environmental Costs of Hyper-Connectivity: Sleeping through Revolution* (2021) Emerald Publishing Ltd: Bingley.

Jordeim, H. and Sandmo, E. (eds) *Conceptualizing the World: An Exploration Across Disciplines* (2018) Berghahn: New York.

Joseph, S. and Castan, M. and *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*" 3ed, (2013) Oxford University Press: Oxford.

Klatt, M. and Meister, M. *Constitutional Structure of Proportionality* (2012) Oxford University Press: Oxford.

Landau, S. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelation" (July/August 2013) *IEEE Security and Privacy* 66.

Loubser, M., Midgley, R. Jabavu, P., Linscott, J. Mukheibir, A. *et al The Law of Delict in South Africa* 3ed (2017) Oxford University Press: Cape Town.

Lyon, D. *Surveillance after Snowden* (2015) Polity Press: London.

Maier, K. *This House Has Fallen: Nigeria in Crisis* (2002) Avalon Publishing: New York.

Malemi, E. *Administrative Law* 3ed (2008) Lagos, Princeton Publishing Co: Lagos.

Mattelart, B. *The Globalisation of Surveillance*" (2010) Polity Press: Cambridge.

McQuiod-Mason, D. *The Law of Privacy in South Africa* (1978) Juta & Co Ltd: Cape Town.

Michael, J. *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) Dartmouth Publishing Ltd: Hampshire.

Miller, R.A. (ed.) *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (2017) Cambridge University Press: Cambridge.

Morozov, E. *The Net Delusion: How not to liberate the world* (2012) Penguin: London

Morsink, J. *The Universal Declaration of Human Rights: Origins, Drafting, and Intent* (1999) University of Pennsylvania Press: Philadelphia.

Morsink, J. *The Universal Declaration of Human Rights and the Holocaust: An Endangered Connection* (2019) George University Press: Washington, DC.

Neethling, J and Potgieter, J. and Knobel, JC. *Law of Delict* 8ed (2021) LexisNexis (Pty) Ltd: Cape Town.

Schabas, W. Nowak's *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2019) Engel Verlag: Germany.

Nwabueze, B.A. *Constitutional History of Nigeria* (1982) Longman Inc.: London.

Nwauche, E. Lindsay D & Ricketson, S "Copyright, Privacy and Digital Rights Management" in Kenyon, A and Richardson, M (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) Cambridge University Press 121.

Obilade, A. *The Nigerian Legal System* (1979) Spectrum Law Series: Lagos.

Okeke, G. *Introduction to Consular Immunities and Privileges, Jurisprudence and Constitutional Law* (2010) Nolix Educational Publications (Nig): Enugu.

Olong, A. *The Nigerian Legal System* 2ed (2007) Malthouse Press: Lagos.

Orwell, G. *Nineteen Eighty-Four* (1950) Signet Classic: New York

Oyediran, O. *The Nigerian 1979 elections* Macmillan International College Editions: Contemporary African Issues Series (1981) Macmillan Nigeria: Lagos.

Pellet, A. "Article 38" in Zimmerman A, Christian, J., Oellers-Frahm, K. and Tomuschat, C. (eds) *The Statute of International Court of Justice: A Commentary* 2ed (2019) Oxford University Press: Oxford.

Shaw, M. *International Law* 9ed (2021) Cambridge University Press: Cambridge.

Shue, H. "Basic Rights: Subsistence, Affluence and U.S Foreign Policy" 2ed (1996) Princeton University Press: Princeton, New Jersey.

Tobi, N. *Sources of Nigerian Law* (1996) MIJ Professional Publishers Limited: Lagos.

Solove, D. *The Digital Person: Technology and Privacy in the Information Age* (2006) New York University Press: New York.

Solove, D. *Understanding Privacy* (2010) Harvard University Press: United States.

Laurens, P. *The Evolution of Human Rights: Visions Seen* (2011), University of Pennsylvania: Pennsylvania.

Stallings, W. and Brown, L. *Computer Security: Principles and Practice* 4ed (2017) Pearson: New York.

Steiner, H. Alston, P and Goodman, R *International Human Rights in Context: Law, Politics, Morals* 3ed (2007), Oxford University Press: Oxford.

Robert, A. and Sivakumaran, S. *The Theory and Reality of the Sources of International Law* in Malcom Evans, ed. *International law* 5ed (2018) Oxford University Press.

Ross, A. "Data Protection Law in South Africa" in Makulilo, AB (ed) *African Data Privacy Laws* (2016) Springer: Switzerland.

Taiwo, A. and Akintola, O. *Introduction to Equity & Trusts in Nigeria* (2016) Princeton and Associates Publishing Company Limited: Lagos.

Thirlway, H. *The Sources of International Law* 2ed (2019) Oxford University Press: England.

Van Dijk, P., Dijk, P. and Hoof, G. *Theory and Practice of the European Convention on Human Rights* (1984) Kluwer Law and Taxation Publishers: Netherlands.

Whitaker, C. (Jr.) *The Politics of Tradition, Continuity and Change in Northern Nigeria, 1946-1966* (2015) Princeton University Press: Princeton, New Jersey.

Zuboff, S. *The Age of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power* (2019) Profile Books: London.

JOURNAL ARTICLES

Abdi, A. "Derogation from Constitutional Rights and Its Implication under the African Charter on Human and People's Rights" 2013 17 *Law Democracy & Development* 92.

Abdulrauf, L. and Daibu, A "New Technologies and the Right to Privacy in Nigeria: Evaluating the Tension between Traditional and Modern Conceptions" 2016 7 *Nnamdi Azikwe University Journal* 113.

Abdulrauf, L. "The Challenges for the Rule of Law Posed by the Increasing Use of Electronic Surveillance in Sub-Saharan Africa" 2018 18 *African Human Rights Law Journal* 369.

Abuza, A. "Constitutional Law: Derogation from Fundamental Rights in Nigeria an Analysis of the Issues Involved" 2016 2 *Port Harcourt Journal of Business Law* 497-519.

Ackermann, L. "Constitutional Comparativism in South Africa" 2006 123 *South African Law Journal* 504.

Adami, R. "Reconciling Universality and Particularity through a Cosmopolitan Outlook on Human Rights" 2012 4 *Cosmopolitan Civil Societies Journal* 24.

Adigun, M. "Enforcing ECOWAS Judgments in Nigeria through the Common Law Rule on the Enforcement of Foreign Judgments" 2019 15 *Journal of Private and International Law* 137.

Aihe, D. "Fundamental Human Rights Provisions as a Means of Achieving Justice in Society" 1973 15 *Malaya Law Review* 42.

Akinola, A. "Nigeria: The Quest for a Stable Polity: Another Comment" 1988 87 *African Affairs* 441.

Alan, D. "The Triangle That Could Square the Circle? The UN International Convention on the Protection of Migrant Workers and Members of Their Families, the EU and the Universal Periodic Review" 2015 17 *European Journal of Migration and Law* 45.

Alexy, R. "The Construction of Constitutional Rights" 2010 4 *Law and Ethics Human Rights* 20.

Andenas, M. and Zleptnig, S. "Proportionality: WTO Law: In Perspective" 2007 42 *Texas International Law Journal* 386.

Aquilina, K. "Public Security versus Privacy in Technology Law: A Balancing Act?" 2010 26 *Computer Law & Security Review* 134.

Arnbak, A. and Goldberg, S. "Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad" 2015 21 *Michigan Telecommunications and Technology Law Review* 360.

Balkin, J. "The Constitution in the National Surveillance State" 2008 93 *Minnesota Law Review* 2.

Banisar, D. "Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information" (2010) 16 *East African Journal of Peace & Human Rights* 125.

Bamberger, K. and Deirdre, K. "Privacy in Europe: Initial Data on Governance Choices and Corporate Practices" 2013 81 *George Washington Law Review* 1532.

Basdeo, V. Montesh, M. and Lekubu, B. "Search for and Seizure of Evidence in Cyber Environments: A Law-Enforcement Dilemma in South African Criminal Procedure" 2014 1 *Journal of Law, Society and Development* 56.

Beaney, W. "The Right to Privacy and American Law" 1966 31 *Law and Contemporary Problems* 254.

Bernal, P. "Data Gathering, Surveillance and Human Rights: Recasting the Debate" (2016) 1 *Journal of Cyber Policy* 243.

Blaauw-Wolf, L. and Wolf, J. "A Comparison between German and South African Limitation Provisions" 1996 *SALJ* 272.

Bigo, D., Carrera, S., Hernanz, N. and Jeandesboz, J. "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law" 2013 61 *Liberty and Security in Europe Papers* 1.

Bilchitz, D. "Privacy, Surveillance and the Duties of Corporations" 2016 *TSAR* 45.

Binder, G. "Cultural Relativism and Cultural Imperialism in Human Right Law" 5 1999 *Buffalo Human Rights Law Review* 211.

Brewster, R. "The Domestic Origins of International Agreements" 2004 44 *Virginia Journal of International Law* 501.

Buchan, A. "Human Rights and the Legitimacy of the International Order" 2008 14 *Legal Theory* 39.

Butler, A. Hidvegi, F., "From Snowden to Schrems: How the Surveillance Debate has Impacted US-EU Relations and the Future of International Data Protection" 2015-2016 17 *Whitehead Journal of Diplomatic & International Relations* 71.

Brems, E. and Adekoya, C. "Human Rights Enforcement by People Living in Poverty: Access to Justice in Nigeria" 2010 54 *Journal of African Law* 258.

Breyer, P. "Telecoms Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR" 2005 11 *European Law Journal* 371.

Burchell, J. "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid" 2009 13 *Electronic Journal of Comparative Law* 12.

Bygrave, L.A. "The Place of Privacy in Data Protection Law" 2001 24 *University of New South Wales Law Journal* 277.

Charney, J. "Universal International Law" 1993 *American Journal of International Law* 529.

Chaudhari, N. and Prasad, S. "Carpenter v United States: State Surveillance and Citizen Privacy" 2019 13 *National Academy of Legal Studies and Research (NALSAR) Student Law Review* 130.

Cho, H. "Rethinking Democracy and Human Rights Education on the Seventieth Anniversary of the Universal Declaration of Human Rights" 2019 20 *Asia Pacific Education Review* 173.

Cohen, T. "But for the Nicety of Knocking and Requesting a Right of Entry: Surveillance Law and Privacy Rights in South Africa" 2000 1 *The Southern African Journal of Information and Communication* 5.

Conway, J. Wu, A and Lipner, S "Guidance on Hand Jewelry for Prevention of COVID-19 Transmission in Healthcare" 2020 33 *Dermatologic Therapy* 1.

Coyle, J. "Incorporative Statutes and the Borrowed Treaty Rule" 2010 50 *Virginia Journal of International Law* 655, 656

Currie, I. "Balancing and the Limitation of Rights in the South African Constitution" 2010 25 *South African Public Law* 411.

Dada, J "Human Rights under the Nigerian Constitution: Issues and Problems" 2012 2 *International Journal of Humanities and Social Sciences* 35.

Dafel, M "The Directly Enforceable Constitution: Political Parties and the Horizontal Application of the Bill of Rights" 2015 31 *SAJHR* 57.

D'Aspremont, J. "The Idea of 'Rules' in the Sources of International Law" 2013 84 *British Yearbook of International Law* 105.

De Baets, A. "The Impact of the 'Universal Declaration of Human Rights' on the Study of History" 2009 48 *History and Theory* 20.

De Bruyn, M. "The Protection of Personal Information (POPI) Act - Impact on South Africa" 2014 13 *International Business and Economics Research Journal* 1315.

Delia-Mihaela, M “Aspects regarding Tortious Civil Liability for the Deeds of Minors” 2021 *Proceedings of the International Conference of Law, European Studies an International Relations Section C* 364.

De Villers, W. “Constitutional Validity of Section 11(a) and (g) of the Drugs and Drug Trafficking-Act: *Minister of Police v Kunjana*” 2017 80 *Journal of Contemporary Roman-Dutch Law* 172.

Deeks, A. “An International Legal Framework for Surveillance” 2015 55 *Virginia Journal of International Law* 295.

Desai, A. “Cybercrime, Cybersurveillance and State Surveillance in South Africa” 2018 31 *Acta Criminologica: South African Journal of Criminology* 149.

Diggelmann, O. and Cleis, M. “How the Right to Privacy Became a Human Right” 2014 14 *Human Rights Law Review* 451.

Engel C. “The Role of Law in the Governance of the Internet” 2006 20 *International Review of Law, Computers & Technology* 201.

Eichensehr, K. “Data Extraterritoriality” 2017 95 *Texas Law Review* 157.

Eijkman, Q. “Access to Justice for Communications Surveillance and Interception: Scrutinising Intelligence-Gathering Reform Legislation” 2018 14 *Utrecht Review* 116.

Elkins, Z. Ginsburg, T and Simmons, B “Getting to Rights: Treaty Ratification, Constitutional Convergence, and Human Rights Practice” 2013 54 *Harvard Law Journal* 75.

Eislen, S. “Fiddling with the ECT Act- Electronic Signatures” 2014 17 *PELR* 2806.

Enabulele, A. “Incompatibility of National Law with the African Charter on Human and Peoples' Rights: Does the African Court on Human and Peoples' Rights have the Final Say” 2016 16 *AHRLR* 22.

Engle, E. “Universal Human Rights: A Generational History 2006 12 *Annual Survey International and Comparative Law* 220.

Ezeanokwasa, J., Ewulum, B. and Mbanugo, O. “Religious Freedom and its Limitation under the 1999 Constitution of Nigeria” 2016 7 *Nnamdi Azikwe University Journal of International Law and Jurisprudence* 63.

Fabbrini, F. "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States" 2015 28 *Harvard Human Rights Journal* 69.

Fura, E. and Klamberg, M. "The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA" in *Freedom of Expression: Essays in Honour of Nicolas Bratza, President of the European Court of Human Rights* 2012, 463.

Finegan, T. "Conceptual Foundations of the Universal Declaration of Human Rights: Human Rights, Human Dignity and Personhood" 2012 37 *Australian Journal of Legal Philosophy* 184.

Fudge, J. "Precarious Migrant Status and Precarious Employment: The Paradox of International Rights for Migrant Workers" 2012 34 *Comparative Labour Law & Policy Journal* 103.

Gane, N. "The Governmentalities of Neoliberalism: Panopticism, Post-Panopticism and Beyond" 2012 60 *Social Review* 611.

Gardocki, L. "Double Criminality in Extradition Law" 1993 27 *Israel Law Review* 289.

Georgieva, I., "The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and its Compatibility with Art. 17 ICCPR and Art.8 ECHR" 2015 31 *Utrecht Journal of International and European Law* 115.

Giliker, P. "A Common Law Tort of Privacy? – The Challenges of Developing Human Rights Tort" 2015 27 *Singapore Academy of Law Journal* 761.

Gligorijevic, J. "A Common Law Tort of Interference with Privacy for Australia Reaffirming *ABC v Lenah Game Meats*" 2021 44 *University of New South Wales Law Journal* 673.

Goldstone, R. "The South African Bill of Rights" 1997 32 *Texas International Law Journal* 467.

Govindjee, A. "Lessons for South African Social Assistance Law from India: Part 1 - The Ties that Bind: The Indian Constitution and Reasons for comparing South Africa with India" 2005 16 *Obiter* 575.

Grainne de Búrca “The Principle of Proportionality and its Application in the EC Law” 1994 13 *The Yearbook of European Law* (YEL) 105.

Granmar, C. “Global Applicability of the GDPR in Context” 2021 11 *International Data Privacy Law* 225.

Hannum, H. “The Status of the Universal Declaration of Human Rights in National and International Law” 1996 25 *Georgia Journal of International and Comparative Law* 317.

Hunter, M. and Smith, T. “Spooked: Surveillance of Journalists in SA” 2018 *Right2Know Campaign* 12.

Hathaway, O. “Do Human Rights Treaties Make a Difference?” 2002 111 *Yale Law Journal* 1935.

Hirsch, D. “The Law and Policy of Online Privacy: Regulation, Self-regulation or Co-regulation?” 2011 34 *Seattle University Law Review* 451.

Heymann, P. “An Essay on Domestic Surveillance” 2016 8 *Journal of National Security and Law & Policy* 428.

Hintz, A. and Brown, I. “Enabling Digital Citizenship? The Reshaping of Surveillance Policy after Snowden” 2017 11 *International Journal of Communication* 788.

Holning, L “Rethinking the Persistent Objector Doctrine in International Human Rights Law 2005 6 *Chicago Journal of International Law* 500.

Hosein, G. Palow, C “Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques” 2013 74 *Ohio State Law Journal* 1071.

Igwe, I. “The Rule of Law and National Security in Nigerian Democracy: A Contemporary Issue under the Aegis of International Law” 2021 7 *Athens Journal of Law* 154-155.

Ikongbeh, J. “Separation of Powers under the Constitution of Nigeria 1999: A Critical Review of its Application since 29th May 1999” 2003 1 *Nigeria Law Journal* 92.

Ilori, T. “Framing a Human Rights Approach to Communications Surveillance Law through the African Human Rights System in Nigeria, South Africa, Uganda” 2021 *African Human Rights Year Book* 134.

Iwobi, A. "Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime" 2016 26 *Transnational Law & Contemporary Problems* 34.

Jackson, V. "Constitutional Law in an Age of Proportionality" 2015 124 *Yale Law Journal* 3096.

Jans, J. "Proportionality Revisited" 2000 27 *Legal Issues of Economic Integration* 241.

Johnson, R. "Strengthening the Monitoring of and Compliance with the Rights of the African Child" 2015 23 *International Journal of Children's Rights* 370.

Kalu, U. "Separation of Powers in Nigeria: An Anatomy of Power Convergences and Divergencies" 2018 9 *NAUJILJ* 117.

Klaaren, J. Breckenridge, K, Cachalia, F, Fonn, S and Veller, M "South Africa's COVID-19 Tracing Database: Risks and Rewards of which doctors should be aware" 2020 110 *South African Medical Journal* 617.

Kokott, J. and Sobotta, C. "The Distinction between Privacy and Data Privacy in the Jurisprudence of the CJEU and EctHR" 2013 3 *International Data Privacy Law* 222.

Koppelman, A. "The Right to Privacy" 2002 *University of Chicago Legal Forum* 105.

King, I. "On-line Privacy in Europe – New Regulation for Cookies" 2003 11 *Journal of Information and Communication Technology Law* 327.

Kumm, M. "The Legitimacy of International Law: A Constitutionalist Framework of Analysis" 2004 15 *The European Journal of International Law* 912.

Lau, H. "Rethinking the Persistent Objector Doctrine in International Human Rights Law" 2005 6 *Chicago Journal of International Law* 501.

Lau, H. "Sexual Orientation: Testing the Universality of International Human Rights Law" 2004 71 *University of Chicago Law Review* 1689.

Lawack-Davids, V.A. "The Interception and Monitoring Bill-Is Big Brother Watching?" 2001 22 *Obiter* 347.

Le, N. "Are Human Rights Universal or Culturally Relative?" 2016 28 *Peace Review* 204.

Li-Ann, T. "Reading Rights Rightly: The UDHR and its Creeping Influence on the Development of Singapore Public Law" 2008 *Singapore Journal of Legal Studies* 268.

Lindgren, J.A. "The Declaration of Human Rights in Postmodernity" 22 2000 *Human Rights Quarterly* 478.

Lim, W. "Assessing the Implications of Digital Contact Tracing for COVID-19 for Human Rights and the Rule of Law in South Africa" 2020 20 *African Human Rights Law Journal* 544.

Loenen, T. "The Equality Clause in the South African Constitution: Some Remarks from a Comparative Perspective" 1997 13 *South African Journal on Human Rights* 401 *South African Journal on Human Rights* 406.

Livingstone, S. and Helsper, E. "Gradiation in Digital Inclusion: Children, Young People and the Digital Divide" 2007 9 *New Media & Society* 671.

Livingstone, S. Carr, J. and Byrne, J. "One in Three: Governance and Children's Rights" 2015 *Global Commission on Internet Governance Paper Series No.22*, Centre for International Governance Innovation: London 5.

Lynskey, O. "Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order" 2014 *International and Comparative Law Quarterly* 569.

Lyon, D. "The Snowden Stakes: Challenges for Understanding Surveillance Today" 2015 13 *Surveillance & Society* 139.

Lyon, D. *Surveillance as Social Sorting: Privacy, Risk and Social Digital Discrimination* (2013) 1.

Macenaite, M. "From Universal towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation" 2017 19 *New Media & Society* 767.

Makulilo, A.B. "A Person is a Person through other Persons – A Critical Analysis of Privacy and Culture in Africa" 2016 7 *Beijing Law Review* 201.

Makulilo, A.B. "Myth and Reality of Harmonisation of Data Privacy Policies in Africa" 2015 31 *Computer Law and Security Review* 79.

Makulilo, A.B. "One Size Fits All": Does Europe Impose its Data Protection Regime on Africa?" 2013 7 *DuD.Datenschutz and Datensicherheit* 447.

Makulilo, A.B. "Privacy and Data Protection in Africa: A State of the Art" 2012 2 *International Data Privacy Law* 164.

Mao, J. and Xi, S. "Article 29(1) of the Universal Declaration of Human Rights: Reflection on Drafting, Sources and influences" 2019 *Cross-cultural Human Rights Review* 53.

Markesinis, B., O'Conneide, C., Fedtke, J. and Hunter-Henin, M., "Concerns and Ideas about the Developing English Law of Privacy (and how Knowledge of Foreign Law might be of Help)" 2004 52 *The American Journal of Comparative Law* 134.

Marx, F.E. and O'Brien, N. "To Regulate or to Over-regulate? Internet Service Provider Liability: The Industry Representative Body in terms of the ECT Act and Regulations" 2011 32 *Obiter* 544.

McCreary, L. "What Was Privacy?" (2008) 86 *Harvard Business Review* 123.

McGonagle, M. "A Tort of Privacy: The Privacy Bill" 2006 1 *Quarterly Review of Tort Law* 1.

Milanovic, M. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" 2015 56 *Harvard International Law Journal* 68.

Manacorda, M and Tesei, A. "Liberation Technology: Mobile Phones and Political Mobilization in Africa" 2020 88 *Econometrica, Economic Society Data* 533.

Modiba, M. "Intercepting and Monitoring Employees' E-mail Communications and Internet Access" 2003 15 *South African Mercantile Law Journal* 363.

Moreham N.A. "Beyond Information: Physical Privacy in English Law" 2014 73 *The Cambridge Law Journal* 350.

Naude, A. and Papadopoulos, S. "Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments" 2016 1 *THRHR* 190.

Neethling, J. "The Concept of Privacy in South African Law" 2005 122 *South African Law Journal* 20.

Loideain, N. "EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era" 2015 3 *Media and Communication* 53.

Niamh, J. "An Analysis of the Extent of the Juvenile Offender's Right to Privacy: Is the Child's Right to Privacy Circumvented by Public Interest?" 2011 19 *European Journal of Crime, Criminal Law and Criminal Justice* 120.

Nomikos, L. "Are We Sleepwalking into a Surveillance Society?" 2017 4 *Bristol Law Review* 113.

Nwauche, E. "The Right to Privacy in Nigeria" 2007 1 *CALS Review of Nigerian Law and Practice* 88.

Nwauche, E. "Law, Religion and Human Rights" 2008 8 *African Journal of Human Rights* 572.

Nwauche, R. "Securing Widow's Sepulchral Rights Through the Nigerian Constitution" 2010 23 *Harvard Human Rights Journal* 141.

Ohlin, J. "Did Russian Cyber Interference in the 2016 Election Violate International Law?" 2017 95 *Texas Law Review* 1579.

Ojo, A. "Separation of Powers in a Presidential System of Government" in 1981 *Public Law Journal* 105.

Orji, U. "The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability" 2018 12 *Masaryk University Journal of Law & Technology* 92.

Ortino, F. "From 'non-discrimination' to 'reasonableness': A Paradigm Shift in International Economic Law?" (April 2005) *Jean Monnet Working Paper 01/05 New York University School of Law* 1.

Okonkwo, D. "The Legal Basis of Freedom of Expression in Nigeria" 1978 8 *California Western International Law Journal* 265.

Philipson G. "Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act" 66 2003 *Modern Law Review* 726.

Plixavra, V. "Centrum for Rättvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy" 2018 4 *European Data Protection Law Review* 567.

Quirine, E. "Access to Justice for Communications Surveillance and Interception: Scrutinising Intelligence-Gathering Reform Legislation" 2018 14 *Utrecht Law Review* 115.

Prosser, W. "Privacy" 1960 48 *California Law Review* 385.

Rautenbach, I.M. "Overview of the Constitutional Court Judgments on the Bill of Rights – 2018" 2019 2 *TSAR* 303.

Rautenbach, I.M. "Proportionality and the Limitation Clauses of the South African Bill of Rights" 2014 17 *Potchefstroom Electronic Law Journal* 2232.

Rautenbach, I.M. "The Limitation of Rights and "Reasonableness" in the Right to Just Administrative Action and the Rights to Access to Adequate Housing, Health Services and Social Security" 2005 4 *TSAR* 628.

Rautenbach, I.M. "The Conduct and Interests Protected by the Right to Privacy" 2001 1 *TSAR* 122.

Richards, N. "Why Data Privacy is (mostly) Constitutional" 2015 56 *William and Mary Law Review* 1506.

Richards, N. "The Limits of Tort Privacy" 2011 9 *Journal on Telecommunications & High Technology Law* 357.

Roberts, A. "Traditional and Modern Approaches to Customary International Law: A Reconciliation" 2001 95 *American Journal of International Law* 757.

Robert-Wray, K. "Human Rights in the Commonwealth" 1968 17 *International and Comparative Law Quarterly* 908.

Robert C. "Three Concepts of Privacy" 2001 89 *Georgetown Law Journal* 2089.

Roehrs, S. "Privacy, HIV/AIDS and Public Health Intervention" 2009 *South African Law Journal* 360.

Ross, A. "Personal Data Protection in New Zealand: Lessons for South Africa?" 2008 *PER* 62.

Ruhs, M. "The Human Rights of Migrant Workers: Why Do So Few Countries Care?" 2012 56 *American Behavioral Scientist* 1280.

Rycroft, A. "A Privacy in the Workplace" (2018) 39 *ILJ* 725.

Sarkin, J. "The Drafting of South Africa's Final Constitution from a Human-Rights Perspective" 1999 47 *American Journal of Comparative Law* 69.

Sanni, A. "Fundamental Rights Enforcement Procedure Rules, 2009 as a tool for the enforcement of the African Charter on Human and Peoples' Rights in Nigeria: The Need for Far-reaching Reform" 2011 11 *African Human Rights Law Journal* 512.

Saurombe, A. "The Role of SADC Institutions in Implementing SADC Treaty Provisions Dealing with Regional Integration" 2012 15 *Potchefstroom Electronic Law Journal* 455.

Schwartz, P. and Solove, D. "Reconciling Personal Information in the United States and European Union" 2014 102 *California Law Review* 877.

Setty, S. "Surveillance, Secrecy, and the Search for Meaningful Accountability" 2015 51 *Stanford Journal of International Law* 69.

Shope, M. "The Adoption and Function of International Instruments: Thoughts on Taiwan's Enactment of the Act to Implement the ICCPR AND the ICESCR" 2012 21 *Indiana International & Comparative Law Review* 163.

Sinha, A. "NSA Surveillance since 911 and the Human Right to Privacy" 2013 59 *Loyola Law Review* 917.

Singh, R. and Strachan, J. "Privacy Postponed" *European Human Rights Law Review Special Edition: Privacy* 25.

Slabbert, M. and Van der Westhuizen, C. "The Possible Effect of the Protection of Personal Information Act 4 of 2013 on Organ and Tissue Donations" 2017 *Obiter* 632.

Sloane, R. "Outrelativizing Relativism: A Liberal Defense of the Universality of International Human Rights" 2001 34 *Vanderbilt Journal of Transnational Law* 531.

Solove, D. "'I've Got Nothing to Hide' and other Misunderstandings of Privacy" 2007 44 *San Diego Law Review* 770.

Taiwo, O. "The Legal Subject in Modern African Law: A Nigerian Report." 2006 7 *Human Rights Review* 24.

Taiwo, E. "Enforcement of Fundamental Rights and the Standing Rules under the Nigerian Constitution: A Need for a more Liberal Provision" 2009 9 *African Human Rights Law Journal* 547.

Taiwo, O. "The Legal Subject in Modern African Law: A Nigerian Report" 2006 7 *Human Rights Law Review* 24.

Tesón, F. "International Human Rights and Cultural Relativism" 25 1985 *Virginia Journal of International Law* 878.

Trachtman, J. "Trade and ... Problems, Cost-Benefit Analysis and Subsidiarity" 1998 9 *European Journal of International Law* 33.

Tzanou, M. "Data Protection as a fundamental right next to privacy? 'Reconstructing' a not so new right" 2013 3 *International Data Privacy Law* 88.

Tzanou, M. "The EU as an Emerging Surveillance Society: The Function Creep Case Study and Challenges to Privacy and Data Protection" 2010 4 *Vienna Online Journal on International Constitutional Law* 409.

Udombana, N. "Mission Accomplished? An Impact Assessment of the UDHR in Africa" 2008 30 *Hamline Journal of Public Law and Policy* 337.

Udombana, N. "Interpreting Rights Globally: Courts and Constitutional Rights in Emerging Democracies" 2005 5 *African Human Rights Law Journal* 55.

Ugochukwu, B. "Balancing, Proportionality, and Human Rights Adjudication in Comparative Context: Lessons for Nigeria" 2014 1 *Transnational Human Rights Review* 1.

Van Wyk, C. "Tuberculosis and the Limitation of Rights in South Africa" 2009 72 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg (THRHR)* 92.

Viljoen, F. "Model Legislation and Regional Integration: Theory and Practice of Model Legislation Pertaining to HIV in the SADC" 2008 41 *De Jure* 384.

Van Niekerk, B. "The Cybersecurity Dilemma: Considerations for Investigations in the Dark Web" 2018 31 *Acta Criminologica: South African Journal of Criminology* 133.

Vian B. "'Veillant Panoptic Assemblage': Mutual Watching and Resistance to Mass Surveillance after Snowden" 2015 3 *Media and Communications* 12.

Ward, J. "Hand Adornment and Infection Control" 2007 16 *British Journal of Nursing* 654.

Warren, S.D. and Brandeis, L. "The Right to Privacy", 1890 4 *Harvard Law Review* at 205.

Westin, A. "Privacy and Freedom" 1967 22 *Administrative Law Review American Bar Association* 487.

Woolman, S. "Out of Order? Out of Balance? The Limitation Clause of the Final Constitution" 1997 *SAJHR* 102.

Weber, R. "The Digital Future-A Challenge for Privacy?" 2015 31 *Computer Law and Security Review* 238.

Yakaré-Oulé, N. Reventlow, Y. and Curling, R. "The Unique Jurisdiction of the African Court on Human and Peoples' Rights: Protection of Human Rights beyond the African Charter" 2019 33 *Emory International Law Review* 204.

Young, J. "Surfing while Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation" 2004 7 *Yale Journal of Law and Technology* 346.

CONFERENCE PAPERS

Ilesanmi, S. Adigun, M and Olatunbosun, A "Economic Rights and Justice: Of Walls and Bridges, Exclusions and Inclusions" Paper presented at conference on Law, Justice and Society, 51st Conference of the Nigerian Association of Law Teachers (NALT) held at Nigerian Law School Bwari, Abuja (July 2018) 118.

Udombana, N. "Constitutional Restructuring in Nigeria: An Impact Assessment" (25 April 2017) Public Lecture delivered at 'Change Nigeria' Lagos, Nigeria 7.

THESES

Abdulrauf, L. *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* (doctoral thesis, University of Pretoria) 2015.

Anucha, D. *The Impact of Constituent Assemblies (1978-1995) on Nigerian Constitutions and Political Evolution* (doctoral thesis, Department of Political Science, Clark Atlanta University), July 2010.

Dafel, M. *The Constitutional Rebuilding of the South African Private Law: A Choice between Judicial and Legislative Law-Making* (doctoral thesis, University of Cambridge) 2018.

Laosebikan, F. *Privacy and Technology Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in Internet Cafes and Suggestions for Appropriate Legislation in Nigeria* (doctoral thesis, Howard College School of Law, University of Kwazulu-Natal, Durban) 2007.

REPORTS

Human Rights Council

Annual Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, 39th session, Agenda items 2 and 3, A/HRC/39/27, 3 August 2018.

Annual report of the Office of the High Commissioner for Human Rights on the Right to Privacy in the Digital age, 28th session, agenda items 2 and 3, A/HRC/28/39, 19 December 2014.

Annual report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the digital age, 27th session, agenda items 2 and 3, A/HRC/27/37, 30 June 2014.

Report of the Special Rapporteur on Artificial Intelligence and privacy, and children's privacy A/HRC/46/37, 25 January 2021.

Report of the Special Rapporteur, A/75/147, Right to privacy (Note by the Secretary-General) 27 July 2020.

Report of the Special Rapporteur on the promotion and protection of human rights...including the right to development on Surveillance and Human Rights, A/HRC/41/35, 28 May 2019.

Report of the UN Special Rapporteur on the right to privacy, A/HRC/40/63, 40th session, agenda item 3, 27 February 2019.

Report of the United Nations Office High Commissioner for Human Rights “Concluding Observations on the Initial Report of South Africa, CCPR/C/125/3/Add.2, 27 April 2016.

Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014.

Report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014.

Report of the UN Special Rapporteur’s on the right to freedom of peaceful assembly and of association A/HRC/26/29 (2014).

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OHCHR, U.N. Doc. A/HRC/23/40 (17 April 2013).

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, OHCHR, A/HRC/13/37, (28 December 2009).

Report of the Office of the High Commissioner for Human Rights on the Right to Privacy, 32nd session, HRI/GEN/1/Rev.9 (I), General comment No.16 par [3], 8 April 1988.

Secretary General’s note on the right to privacy, Item 75(b), A/76/220, 23 July 2021
UN General Assembly resolution on the right to privacy in the digital age, 42nd session, A/HRC/42/L.18, 24 September 2019.

UN General Assembly resolution on the right to privacy in the digital age, 28th session, A/HRC/RES/28/16, 23 March 2017.

United Nations General Assembly Resolution on the Right to Privacy in the digital age, 71st session, agenda 68 (b), A/RES/71/199, 25 January 2017.

United Nations General Assembly Resolution on the Right to Privacy in the digital age, 69th session, agenda 68 (b), A/RES/69/166, 10 February 2015.

United Nations General Assembly Resolution on the Right to Privacy in the digital age, 68th session, agenda 69(b), A/RES/68/167, 21 January 2014.

UN Human Rights Committee (HRC), *General comment no. 34, Article 19, Freedoms of opinion and expression*, 12 September 2011, CCPR/C/GC/34.

South Africa

Annual report on interception of private communications to the Joint Standing Committee on Intelligence by Justice Nkabinde (17 March 2021).

South African Law Commission “Discussion Paper 109, Project 124 on Privacy and Data Protection” (October 2005).

United Kingdom

Straw “*Interception of Communication in the United Kingdom*” A Consultation Paper Presented by the Secretary of State for the Home Department by Command of Her Majesty (June 1999).

United States of America

Report of the Secretary’s Advisory Committee on Automated Personal Data Systems: United State Department of Health, Education and Welfare (25 July 1973) *Library of Department of Justice*.

ONLINE RESOURCES

African Court in Brief African Court on Human and Peoples' Rights, <http://www.african-court.org/en/index.php/2-uncategorised/47-african-court-in-brief> (accessed 2019-06-12).

Agbu, C “Worked to the Grave: Neglect of Work-Life Balance maybe Killing Judges” (9 November 2021) *Legal Business Day* <https://legal.businessday.ng/2021/11/11/worked-to-the-grave-neglect-of-work-life-balance-may-be-killing-judges/> (accessed 2021-12-01).

Akinkuotu “Banditry: Months after “no fly order”, FG shuts down telecom sites in Zamfara” (4 September 2021), <https://punchng.com/banditry-months-after-no-fly-order-fg-shuts-down-telecom-sites-in-zamfara/> (accessed on 2022-02-24).

Aljazeera News “Nigerian Ends its Twitter Ban after Seven Months” (12 January 2022), <https://www.aljazeera.com/economy/2022/1/12/nigeria-ends-its-twitter-ban-after-seven-months> (accessed on 2022-02-20).

American Civil Liberties Union, *Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy Under Article 17 of the International Covenant on Civil and Political Rights* (2014) <https://www.aclu.org/other/human-right-privacy-digital-age> (accessed 2019-06-06).

Amnesty International “#ENDSARS Movement: From Twitter to Nigerian Streets” <https://www.amnesty.org/en/latest/campaigns/2021/02/nigeria-end-impunity-for-police-violence-by-sars-endsars/> (accessed on 2022-03-15).

Article 18 (Freedom of Thought, Conscience or Religion), 30 July 1993, CCPR/C/21/Rev.1/Add.4, <https://www.refworld.org/docid/453883fb22.html> (accessed on 2021-02-10).

Babalola, O. “Data Protection and Privacy Challenges in Nigeria (Legal Issues)” <https://olumidebabalolalp.com/privacy-challenges-nigeria/> (accessed 2021-03-03).

Bawa, N. “The Regulation of Interception of Communication and Provision of Communication-Related Information Act” <http://thornton.co.za/resources/telelaw13.pdf> (accessed 2020-03-30).

Bergen, P. “September 11 Attacks” <https://www.britannica.com/event/September-11-attacks> (accessed 2022-11-21).

Blumberg, A.J. and Eckersley, P. “On locational privacy, and how to avoid losing it forever” (August 2009) *White Paper, Electronic Frontier Foundation* <https://www.eff.org/files/eff-locational-privacy.pdf> (accessed on 2021-04-23).

Cannataci, J. “Working Draft Legal Instrument on Government-Led Surveillance and Privacy” (28 February 2018) https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf (accessed on 2019-10-21).

Chima, O. "Democracy in Danger: Law of Sedition and the Idea of Free Press" https://www.academia.edu/12981450/Democracy_in_danger_law_of_sedition_and_the_idea_of_a_free_press (accessed on 2021-03-01).

Crockford, K "Graphs by MIT Students Show the Enormously Intrusive Nature of Metadata" (7 January 2014) www.aclu.org/blog/national-security/secrecy/graphs-mit-students-show-enormously-intrusive-nature-metadata (accessed on 2020-01-30).

Dell'Antonia, K.J "Don't Post about Me on Social Media, Children Say" *The New York Times* (March 8, 2016) <https://archive.nytimes.com/well.blogs.nytimes.com/2016/03/08/dont-post-about-me-on-social-media-children-say/> (accessed 2019-03-10).

Document of the OHCHR "Convention on the Right of a Child" <https://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf> (accessed 2018-11-11).

Document of the OHCHR "International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families" <https://www.ohchr.org/Documents/ProfessionalInterest/cmw.pdf> (accessed 2018-11-11).

Dodd "Government's Defence of Surveillance Unconvincing says ex-watchdog" (2014-06-18) *The Guardian*, <https://www.theguardian.com/world/2014/jun/18/government-surveillance-watchdog-loopoles> (accessed 2019-03-03).

Draft Report, Addis Ababa Ethiopia: African Union (2008), https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/2_Draft_Report_Study_on_Telecom_ICT_Policy_31_March_08.pdf (accessed 2019-2-11).

Executive Office of the President "Big Data and Privacy: A Technological Perspective" (1 May 2014) <https://obamawhitehouse.archives.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy> (accessed 2021-06-10).

Farrel "History of 5-Eyes-Explainer" (2 December 2013) <https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer> (accessed 2018-10-11).

Global Conflict Tracker “Boko Haram in Nigeria” (11 March 2022) <https://www.cfr.org/global-conflict-tracker/conflict/boko-haram-nigeria> (accessed on 2022-03-13).

Hunter “Track and Trace, Trial and Error: Assessing South Africa’s Approaches to Privacy in Covid-19 Digital Contact Tracing” *The Media Policy and Democracy Project* (November 2020) https://www.researchgate.net/publication/350896038_Track_and_trace_trial_and_err_or_Assessing_South_Africa%27s_approaches_to_privacy_in_Covid19_digital_contact_tracing (accessed 2021-09-10).

Igwe, O.W and Alunegbe, A., “The Law of Sedition in Contemporary Nigerian Criminal Law: A Review of the Case of Arthur Nwankwo v The State” (July 2018) https://www.researchgate.net/publication/326380881_The_Law_of_Sedition_in_ContemporaryNigerian_Criminal_Law_A_Review_of_the_Case_of_Arthur_Nwankwo_v_The_State (accessed on 2021-03-01).

International Justice Resource Center “Court of Justice of the European Union” <https://ijrcenter.org/regional-communities/court-of-justice-of-the-european-union/> (accessed on 2019-03-28).

International Institute for Democracy and Electoral Assistance “Limitation Clauses” (November 2014) https://constitutionnet.org/sites/default/files/limitations_clauses.pdf (accessed 2021-02-01).

Interview with the Retired Chief Registrar of the Supreme Court, Mrs Hadizatu Uwani Mustapha “With 10, 000 Pending Appeals, the Supreme Court is Overworked” (17 August 2021) *This Day Newspaper* <https://www.thisdaylive.com/index.php/2021/08/17/with-10000-pending-appeals-the-supreme-court-is-overworked/> (accessed 2021-12-01).

Ishiekwene, A “Lawyers, Buhari and the Ruins of Law” (31 August 2018) *Vanguard News* <https://www.vanguardngr.com/2018/08/lawyers-buhari-and-the-ruie-of-law/> (accessed 2021-08-06).

Irei, A. “Guide to Building an Enterprise Unified Communications Strategy” <https://searchunifiedcommunications.techtarget.com/definition/real-time-communications> (accessed 2021-10-24).

Rozen, J. "How Nigeria's police used telecom surveillance to lure and arrest journalists" (13 February 2020) *Committee to Protect Journalists* <https://cpj.org/2020/02/nigeria-police-telecomsurveillance-lure-arrest-journalists/> (accessed 27 December 2022).

Manohar v Union of India, Supreme Court of India, Writ Petition (Criminal) No. 314 of 2021, 27 October 2021 [file:///Users/tope/Downloads/Manohar Lal Sharma vs Union Of India on 27 October 2021. PDF](file:///Users/tope/Downloads/Manohar%20Lal%20Sharma%20vs%20Union%20Of%20India%20on%2027%20October%202021.PDF) (accessed on 2022-01-03).

Mare, A. and Duncan, J. "Report compiled on An Analysis of the Communications Surveillance Legislative Framework in South Africa" (November 2015) https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (accessed 2020-02-03).

Marczak, B., Scott-Railton, J., Siddharth, P., Siena, A. and Deibert, R. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles" (1 December 2020) *Citizens Lab Research Report No. 133, University of Toronto* <https://tspace.library.utoronto.ca/bitstream/1807/106212/1/Report%23133--runningincircles.pdf> (accessed on 2022-08-01).

Miniwatts Marketing Group, Internet World Stats "Internet Usage Statistics for Africa" (June 30, 2019) <http://www.internetworldstats.com/stats1.htm> (accessed 2019-07-28).

National Information Standards Organization, "Understanding Metadata," (2004) NISO Press at <https://www.niso.org/publications/understanding-metadata-2017> (accessed 2021-01-10).

Nigeria ratified the Protocol to the ACHPR on 20 May 2004 [https://au.int/sites/default/files/treaties/36393-sl-PROTOCOL TO THE AFRICAN CHARTER ON HUMAN AND PEOPLES RIGHTS ON THE ESTABLISHMENT OF AN AFRICAN COURT ON HUMAN AND PEOPLES RIGHTS.pdf](https://au.int/sites/default/files/treaties/36393-sl-PROTOCOL%20TO%20THE%20AFRICAN%20CHARTER%20ON%20HUMAN%20AND%20PEOPLES%20RIGHTS%20ON%20THE%20ESTABLISHMENT%20OF%20AN%20AFRICAN%20COURT%20ON%20HUMAN%20AND%20PEOPLES%20RIGHTS.pdf) (accessed on 2018-12-28).

"Nigerians support Anti Same-sex Bill" (20 June 2013) <https://www.vanguardngr.com/2013/06/nigerians-support-an> (accessed 2021-01-27).

Nyst “The Five Eyes Fact Sheet”, Privacy International (26 November 2013) <https://privacyinternational.org/news-analysis/1204/five-eyes-fact-sheet> (accessed 2018-10-01).

Mare, A. and Duncan, J. “Report compiled on An Analysis of the Communications Surveillance Legislative Framework in South Africa” (November 2015) https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (accessed 2020-02-03).

Ojo “No to Monitoring of Nigerian’s Communications” (20 October 2021) *Punch Newspaper* <https://punchng.com/no-to-monitoring-of-nigerians-communications/> (accessed on 2022-02-19).

Onwuaso “Paradigm Initiative Challenges Nigerian Government’s Surveillance of Social Media” (29 January 2018) <https://www.nigeriacommunicationsweek.com.ng/paradigm-initiative-challenges-nigerian-governments-surveillance-of-social-media/> (accessed 2022-04-11).

Parliament of the Republic of South Africa “Annual Report of the Joint Standing Committee on Intelligence for the Financial Year Ending 31 March 2016” (13 December 2016) <http://pmg-assets.s3-website-eu-west-1.amazonaws.com/intelligence.pdf> (accessed 2020-03-22).

Privacy international explanatory document on phone monitoring (May 2018) <https://privacyinternational.org/explainer/1640/phone-monitoring> (accessed 2019-02-01).

Privacy International <https://privacyinternational.org/education/data-and-surveillance> (accessed on 2020-01-30).

Report of the Experts Session of the Extraordinary Conference of African Union Ministers in Charge of Communication and Information Technologies (CITMC), http://registry.africa/wpcontent/uploads/2017/06/CITMC_ExpertsReport_ORTambo.pdf (accessed on 2018-10-17).

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, April 17, 2013, https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed on 2019-10-21).

Rozen, J. “How Nigeria’s Police used Telecom Surveillance to Lure and Arrest Journalists” (13 February 2020) *Committee to Protect Journalists* <https://cpj.org/2020/02/nigeria-police-telecom-surveillance-lure-arrest-journalists/> (accessed 2020-08-01).

Samarajiva and Perera-Gomez “Bulk Data: Policy Implications (Draft)” (2018) <https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56922/56971.pdf> (accessed 2020-03-18).

Siracusa Principles (April, 1985) <https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf> (accessed 2019-06-10).

Silva, D.S and Smith, M.J “Commentary: Limiting Rights and Freedoms in the Context of Ebola and Other Public Health Emergencies: How the Principle of Reciprocity Can Enrich the Application of the Siracusa Principles” (2 June 2015) *Health and Human Rights* <https://www.hhrjournal.org/2015/06/commentary-limiting-rights-and-freedoms-in-the-context-of-ebola-and-other-public-health-emergencies-how-the-principle-of-reciprocity-can-enrich-the-application-of-the-siracusa-principles/> (accessed 2021-02-08).

South African Law Commission “Discussion Paper 109, Project 124 on Privacy and Data Protection” (October 2005) <https://www.justice.gov.za/salrc/dpapers/dp109.pdf> 5 (Chapter 2) (accessed 2019-04-10).

South African Law Commission “Discussion Paper 109, Project 124 on Privacy and Data Protection” (October 2005) <https://www.justice.gov.za/salrc/dpapers/dp109.pdf> 5 (Chapter 2) (accessed on 2020-2-11).

Sub-regulation 13 of GN. 43199; “Minister Ronald Lamola appoints Justice Kate O’regan as Coronavirus COVID-19 Designated Judge” (3 April 2020) <https://www.gov.za/speeches/minister-ronald-lamola-appoints-justice-kate-o’regan-coronavirus-covid-19-designate-judge-3> (accessed 2021-04-24).

The Constitution of the Federal Republic of Nigeria, 1979 https://constitutionnet.org/sites/default/files/nig_const_79.pdf (accessed on 2021-02-15).

The head of argument of the plaintiffs in *AmaBhungane v Minister of Justice* https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf (accessed 2020-08-10).

Tomuschat, C “International Covenant on Civil and Political Rights” http://legal.un.org/avl/pdf/ha/iccpr/iccpr_e.pdf (accessed on 2018-10-01).

United Nations document “The Right to Privacy in the Digital Age” <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx> (accessed 5 November 2018).

United Nations Factsheet No. 30, OHCHR, the UN Human Rights Treaty System: An Introduction to the Core Human Rights Treaties and the Treaty Bodies <https://www.ohchr.org/sites/default/files/Documents/Publications/FactSheet30Rev1.pdf> (accessed 2018-12-07).

United Nations Human Rights Office of the High Commissioner, “International Covenant on Civil and Political Rights” (1996-2018) <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> (accessed 2018- 10-01).

United Nations, “Member States” <https://www.un.org/en/about-us/member-states> (accessed on 2018-12-7).

Watney, M “State-On-Nationals’ Electronic Communication Surveillance in South Africa: A Murky Legal Landscape to Navigate?” (2015) https://digifors.cs.up.ac.za/issa/2015/Proceedings/Full/3_Paper.pdf (accessed on 2020-01-10).

Welekwe, A. “Demystifying Circles 3G mobile phone snooping technology” (18 June 2016) <https://www.premiumtimesng.com/business/business-interviews/205494-demystifying-circles-3g-mobile-phone-snooping-technology-can-protect-privacy-amakiri-welekwe.html?tztc=1> (accessed 2023-01-30).

