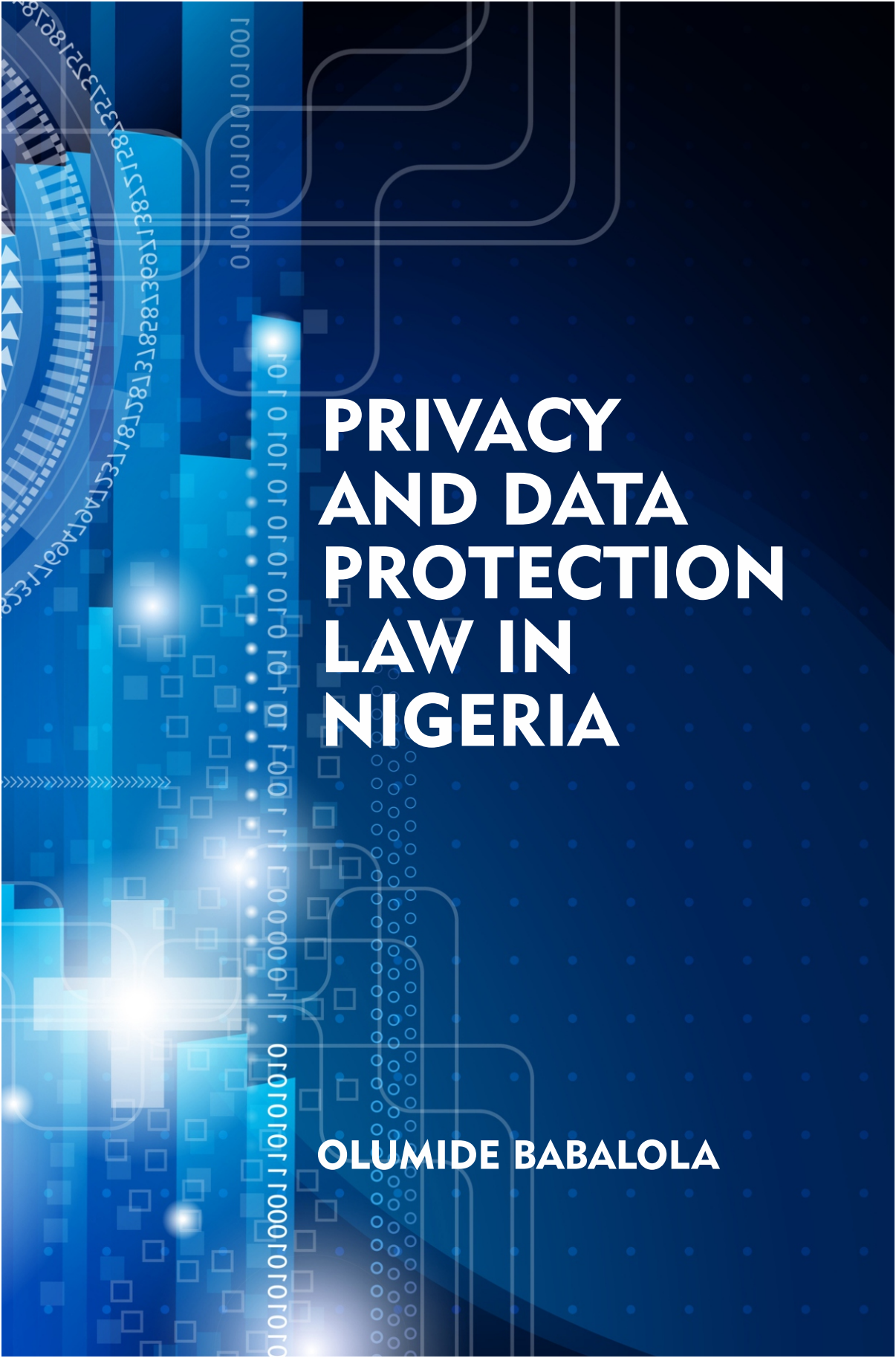
PRIVACY AND DATA PROTECTION LAW IN NIGERIA
OLUMIDE BABALOLA

PRIVACY AND DATA PROTECTION LAW IN NIGERIA

OLUMIDE BABALOLA

Privacy and Data Protection Law in Nigeria

ISBN: 978-978-996-459-8

First Published 2021

Publisher's Contact Details
Noetico Repertum Inc.
12 Berkeley Street, Off King George V Road,
Moloney, Lagos Island, Lagos, Nigeria.
0812 356 7055

Printed in Nigeria by
CI PLUS Limited
Block C, 2nd Floor Adebowale House,
150 Ikorodu Road, Onipan, Lagos
T: 0802 320 7248, 0802 999 3189
info@ciplusonline.com,
www.ciplusonline.com

Contents

Part IV: Nigerian Data Protection Regulation: The Processing of Personal Data

Part V: Rights, Supervision and Enforcement

Preface

Until the tech bubble hit Nigeria in the dawn of the millennium, the country's legislature and policymakers were not really concerned about privacy outside the home as it was generally taken for granted that citizens did not have reasonable expectation of privacy in public places. Apart from the cosmetic replication of right to private and family life in successive constitutional documents, the dimensions of the all–important right to privacy and its extension to informational privacy were neither legislatively explored nor guaranteed. Hence, the other shades of right to privacy neither received considerable attention in the classrooms nor courtrooms. Since Nigeria's independence in 1960, less than seventy decisions have been given by the Court of Appeal and Supreme Court on the right to privacy and no law textbook has been written on the subject even though privacy ought to be taught under constitutional law or human rights law in the universities.

Nevertheless, starting from 2007, the right to privacy began to surface in other statutes when the National Identity Management Commission Act was passed with some privacy provisions embedded in it. However, informational privacy (data protection) effectively appeared for the first time in a legislation, (albeit subsidiary) when the Nigerian Communications Commission (NCC) released the Consumer Code of Practice Regulations in

2007 even though there exists no record of its judicial or quasi–judicial enforcement at the appellate courts.

Consequently, other subsidiary legislation followed suit by making provisions for data protection principles however, the subject was not taken seriously until the release of Nigeria Data Protection Regulation (NDPR) in January 2019 by the National Information Technology Development Agency (NITDA) which now plays the role of Nigeria's data protection authority. The release of NDPR has not only increased many more Nigerians' interest in data protection, it has also effectively opened up a new practice area for lawyers. It will also introduce a new subject for law students when the universities eventually embrace privacy and data protection as part of their curriculum like their contemporaries in Tanzania and South Africa.

This new practice area came with the anticipated need for (academic) resources to aid practitioners in the field and guide students in the classrooms which vacuum inspired my *Casebook on Data Protection* in 2020–a compilation of 144 decisions of the European courts on varying issues bordering on privacy and data protection. The casebook is explicably populated by foreign decisions because at the time of its publication, no Nigerian court had given a decision on data protection (strictly so called) and while introducing the casebook, I admit that the book will 'momentarily fill the unmistakable knowledge gap pending the arrival of worthier scholarly books addressing the subject in a more comprehensive and interrogative style'. This book seeks to fulfil that promise on my part while I respectfully hope other academics or practitioners will also contribute to the body of knowledge by publishing more textbooks on privacy and data protection in Nigeria.

This book prides itself as the first Nigerian law textbook on the right to privacy and it is divided into six parts with twenty–two chapters. The first part reproduces the various academic definitions of privacy right from the very first attempt by Samuel Warren and Louis Brandeis in their 1890 article, as well as the taxonomy and typology of privacy in Nigeria. It also examines privacy as a tort under the statutes and as a fundamental right under the extant Constitution respectively.

Part two discusses evolution and sources of data protection law in Nigeria as well as the relationship between data protection and other rights while the third part introduces the Nigeria Data Protection Regulation (NDPR) in the light of right to data protection and conceptual definitions of data protection terminologies under the regulation. The fourth part examines the principles of data protection, lawful bases for data processing, derogations and exemptions, processing of sensitive data and data security while the fifth part discusses data subjects' rights, data protection authority, enforcement of data protection, administrative fine and damages and the concluding part examines international transfers of data, data breaches and suggested reforms.

This book was inspired and moulded by a number of people and events. I am grateful to my immediate family members (My wife and kids–Ajibike, Moyinoluwa and Mofeoluwa Babalola) for creating an enabling environment to conclude the manuscript while simultenously attending classes for my LLM at the University of Reading. Special thanks also to my parents–Deacon D.K & Pastor N.A. Babalola as well as my siblings. I am greatly indebted to Prof. Alex B. Makulilo, Africa's most prolific academic on data protection, for shaping the table of contents without which the publication of this book might have been delayed. I am also thankful for the editorial tutelage I received from

Dr. Adrian Aronsson–Storrier and Dr. Bolanle Adebola both Associate Professors at the University of Reading, United Kingdom. I am also grateful to Prof. E.S. Nwauche of University of Fort Hare, Dr. Basak Bak of University of Reading, Prof. Yinka Olomojobi of Babcock University and Dr. Samuel I. Nwankwo of Leibniz Universitat, Hannover for taking out time to advise on the draft manuscript of this book. Special recognition to Seun (Salako) Osuji, Joy Eguaoje, Ayodele Okedele, Oladotun Owoyemi and Laide Awaiye for helping with the manuscript and typesetting.

Ultimately, I accept full responsibility for all errors and inadequacies of this book while modestly believing that its contents would nevertheless contribute to the already mounting body of knowledge in the field of privacy and data protection in Nigeria.

Respectfully,
Olumide Babalola
School of Law
University of Reading
Whiteknights
Reading, Berkshire
United Kingdom
olumide@oblp.org
8 September 2021.

CHAPTER ONE

Definition of Privacy

Privacy is an inherently nebulous and problematic concept. It is incapable of any precise or generally acceptable definition, hence, researchers have described rather than define the phenomenon.[1] For all intents and purposes in this book, the word 'privacy' is used interchangeably with the concept of 'right to privacy' which is related but distinct from the former. The twin concept is usually confused but the difference may be alluded as a 'chicken and egg' situation–if there exists a right to privacy, then 'privacy' is the object of that right.[2] Parent says privacy is in 'conceptual shambles'[3] but Stephen concludes that it is impossible to define privacy but it can be described.[4]

Judge Biggs referred to privacy as 'haystack in a hurricane,'[5] and to Miller, it is 'exasperatingly vague and evanescent,'[6] while Moore says, it is 'a difficult notion because rituals of association and disassociation are cultural and species–relative.'[7] In his attempt at conceptualising privacy, Thompson says nobody seems to have any clear idea what it is'[8] and in Wacks' voyage of discovery, he resolved that, the search for definition of privacy has

1 Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press, Cambridge, 1971) 262.
2 See Bjorn Lundgren 'A Dilemma for Privacy as Control' (2020) 24 The Journal of Ethic, 165–175.
3 William A. Parent 'A New Definition of Privacy for the Law' (1983) 2(3) Law and Philosophy 305–338.
4 James Fitzjames Stephen, 'Liberty, Equality, Fraternity (1st ed., Smith, Elder & Co., London, 1873).
5 Ettore v Philco Television Broadcasting Corp. 229 4.21 481 (3rd Circ.).
6 Athur Miller, The Assault on Privacy, (University of Michigan Press, Ann Arbor, 1971).
7 Adam Moore, Defining Privacy' (2008) 39(3) Journal of Social Philosophy, 411–428.
8 Judith Jarvis Thompson, The Right to Privacy' (1975) 4(4) Philosophy & Public Affairs, 295.

produced sterile and futile debate. [9] Marmor however found it as a curious kind of right[10] whereas Solove says privacy is a 'concept in disarray,[11] Scheppele laments that the concept suffers from 'embarrassment of meaning'[12] and Gerety says, 'privacy is capable of representing everything and anything to every proponent.'[13] Zimmerman says privacy is neither here nor there since the concept has almost as many meanings as 'Hydra had heads'[14] and Gutwirth observes that, the notion of privacy remains out of the grasp of every academic chasing it and will still remain elusive.[15] Bennet found that, attempts to define privacy have not met with any success[16] while Whitman described it as unusually slippery concept.[17]

Privacy has however been viewed from inter–disciplinary perspectives. In constitutional law, it is often approached from the realm of personal autonomy and freedom to make certain personal decisions and to engage in some self–serving activities. In Economics, issues of privacy arise over private information divulged during transactions and concerns over free movement of personal data.[18] The Anthropologists in their competitive nature, misuse personal information to the detriment of the individuals for some personal gains with its privacy implications.[19]

9 R. Wacks, The Protection of Privacy (Sweet & Maxwell, London, 1980).
10 Andrei Marmor 'What is Right to Privacy?' (2015) 43(1) Philosophy and Public Affairs, 3–26.
11 Daniel Solove, *Understanding Privacy* (Harvard University Press, Cambridge, 2008) 1.
12 Kim Lane Scheppele, Legal Secrets, Equality and Efficiency in the Common Law (University of Chicago Press, Illinois, 2020).
13 Tom Gerety, 'Redefining Privacy' (1977) 12 Horv C.R.C.L.L. Rev. 233 at 234.
14 Dale Zimmerman 'False Light Invasion of Privacy: The Light that Failed' (1989) 64 New York University Law Review, 375–83
15 Serge Gutwirth, *Privacy and the Information Age* (Rowman & Littlefield, Maryland, 2002) 30.
16 Colin J. Bennet, *Regulating Privacy Data Protection and Public Policy in Europe and United States* (Cornel University Press, Newyork, 1992) 288.
17 James Whitman, 'The Two Western Culture of Privacy: Dignity Versus Liberty' (2004) 77 The Yale Law Journal, 475: See also Demetrius Klifou, Privacy–Invading Technologies, and Privacy by Design (Springer Publishing, New York, 2004).
18 George Stigler, 'An Introduction to Privacy in Economics and Politics' (1980) 9(4) The Journal of Legal Studies, 623–644.
19 Sjaak van der Geest 'Privacy from an Anthropological Perspective' in Bart van der Sloot and Aviva de Groot (eds)*The Handbook of Privacy Studies* (Amsterdam University Press, Amsterdam, 2018).

The philosophers have theorised privacy and identified many value systems as seen from many perspectives and context–based definitions.[20] In psychology, they have linked privacy to an individual's self–esteem which makes him appreciate and view himself in a different light from others.[21]

Regardless of the perceived difficulty of definition, researchers have succeeded in describing and identifying the concept of privacy in terms of relative utilities and expectations. On the antique nature of privacy, Rengel says 'references to the concept of individual privacy have been prevalent since the inception of civilisation. The concept of privacy is mentioned in the Code of Hammurabi, the Bible, the Qur'an, Jewish law, and was present in classical Greece and ancient China. The need for privacy is not limited to certain cultures, and most societies regard some areas of human activity as being unsuitable for general observation and knowledge.'[22]

Moore approached privacy in a rather descriptive or normative term theorising that the concept has been variously viewed from different perspectives that have coloured its definitions or descriptions over the years and thereby compounded its chameleonic nature. [23] DeCew identified two major schools of thought that have conceptualized privacy into 'reductionism' and 'coherentism.'[24] The reductionists have posited that, there is no such distinct right as privacy and that it stems from other related

20 Herman T. Tavani, 'Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy' (2007) 38(1) Metaphilosophy, 1–22.
21 Avelie Stuart, Arosha K. Bandara and Mark Levine, 'The Psychology of Privacy in the Digital Age' (2019) 13 (6) Social and Personality Psychology Compass, 1.
22 Alexandra Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2014) 2(2) Groningen Journal of International Law, 34.
23 Adams Moore, 'Defining Privacy' (2008) 139(3) Journal of Social Philosophy, 412.
24 Judith De Cew, 'Privacy' (2018) The Stanford Encyclopaedia of Philosophy, <https://plato.stanford.edu/entries/privacy/> accessed 3 April 2021.

rights, hence the concept is of little or no utilization value[25] while to the reductionists, rather than accord privacy the consideration of fundamental rights and norms, it may be approached as other more basic rights like proprietary rights.[26] Some even argued that, privacy was created out of nowhere without constitutional foundation.[27]

The coherentism proponents conceded to the relationship between privacy and other rights but maintained its distinction from such concepts on the theory that, it is a stand–alone right. They posit that right to privacy coherently and distinctively guarantees every human with a degree of personal autonomy over various aspect of his life.[28]

The concept of privacy has been defined from many view points since the eighteenth century when the idea was first mooted[29] by two American lawyers (Samuel Warren and Louis Brandeis) who defined the concept as 'the right to be let alone.'[30] Their intervention was however aimed at conceptualizing a cause of action for invasion of privacy especially from tortious claim's point

25 David Matheson, 'A Distributive Reductivism About the Right to Privacy' (2008) 9(1) The Monist, 108–129; Robert Posner, The Economics of Justice (Hup, Cambridge 1981); Judith Jarvis Thompson, 'The Right to Privacy' Philosophy & Public Affairs 4(1975) 295–314; Paul Freund, Privacy: One Concept or Many in Privacy & Personality (1st edn Routledge, London, 1971).

26 Benedict Rumbold and James Wilson, 'Privacy Rights and Public Information' (2019) 27(1) The Journal of Philosophy and Public Affairs 269–288; William A. Parent, 'Privacy, Morality and the Law' (1983) 12 Philosophy and Public Affairs, 269–288.

27 Robert Bork, *The Tempting of America: The Political Seduction of the Law* (Free Press, New York, 1990)

28 Andrei Marmor 'what is Right to Privacy' (2015) 43(1) Philosophy Public Affairs, 6.

29 Some researchers have however accounted that it was Sir F.J. Stephen that first conceptualized privacy two decades before Warren and Brandies in his book–James Fitzjames Stephen, 'Liberty, Equality, Fraternity (1st ed., Smith, Elder & Co., London, 1873). Schoeman accounted that, Fitzjames Stephen (the Jurist), Henry James (Journalist) and E.L Godkin had prior to the lawyers, written on the concept of privacy. See Ferdinand d. Schoeman, 'Privacy Philosophical Dimensions' (1984) 21 PIHL Q 199, 202–03.

30 Samuel Warren and Louis Brandeis 'The Right to Privacy' (1896) 4(5) Harvard Law Review, 193–220. The 'right to be let alone' was an adaptation from an adaptation of Cooley's exposition in his book on torts. See Thomas M. Cooley, *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract* (Callaghan and Company, Chicago, 1879). The article was written as an academic response to and disapproval of the embarrassing newspaper coverage of some social events that Warren's wife held, especially their daughter's wedding. See William L. Prosser, 'Privacy', A Legal Analysis' (1960) 48 California Law Review 338–423; Paolo Guarda, 'Data Protection, Information Privacy, and Security Measures: An Essay on the European and the Italian Legal Frameworks' (2008) < https://core.ac.uk/download/pdf/150082461.pdf> accessed 12 April 2021.

of view.[31] Carolan views it as the 'notion that individuals enjoy an enforceable entitlement to respect for their private lives.'[32] An individual enjoys privacy in any circumstance in which he/she is guaranteed protection from intrusion, interference and informal access[33] which right Margulis defines as the 'selective control over transactions between self (or one's group) and others, the ultimate aim of which is to enhance autonomy and/or to minimise vulnerability.'[34]

Gerety prefers to address privacy as a nominative concept of 'autonomy or control over the intimacies of personal identity. According to him, autonomy, identity and intimacy are all necessary and together normally sufficient for the proper invocation of the concept of privacy.[35] In an attempt to further understand the concept of privacy, Mai even advised a shift from definitions of privacy to models of privacy[36]and in the same vein, Winslade and Ross see privacy as freedom from external intrusion or freedom from external prohibition.[37]

Parker describes it as 'control over when and by whom the various parts of us can be sensed by others.'[38] Fried posits that privacy is 'not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.'[39] To Altman, privacy is the selective control of access

31 Thomas Emerson, 'The Right of Privacy and Freedom of the Press' (1979) 14(2) Harvard Civil Rights for Law Reviews, 330.
32 Eoin Carolan 'The Concept of a Right to Privacy' in Hillary Delancy and Eoin Carolan. (eds) *The Right to Privacy: A Doctrinal and Comparative Analysis* (Thomson Round Hall, Dublin, 2008).
33 Herman Tarvani, 'Philosophical Theories of Privacy: Implication for an Adequate Online Privacy Policy' (2007) 38(1) Metaphilosophy, 1.
34 Stephen T. Margulis, 'Conceptions of Privacy: Current Status and Next Steps' (1977) 33(3) Journal of Social Issues, 5.
35 Tom Gerety, 'Redefining Privacy (1977) 2 Harv CRCLL Rev. 233 at 236
36 Jens–Erik Mai, 'Three Models of Privacy, New Perspectives on Informational Privacy' (2016) 37(1) Nordicom Review 171–175.
37 William J. Winslade and Judith Ross, 'Privacy Confidential and Autonomy in Psychotherapy' (1985) 64 (4) Nebraska Law Review, 580.
38 Richard Parker, A Definition of Privacy (1st edn Routledge, London, 2001) 1.
39 Charles Fried 'Privacy' (1968) 77(3) The Yale Law Journal 475–493.

to the self, involving dialectic, optimization and multimodal process.[40] Scholz simply says it is an individual's right to have control over his personal information or data.[41]

Cohen defines the concept as 'the shorthand for breathing room to engage in the processes of boundary management that enables and constitute self–development so understood, privacy is fundamentally dynamic'[42] Allen defines privacy as 'personal data control or rights of data control; that the right of privacy is a right of personal data control; and that enhancing personal data control by individuals is the optimal end of privacy regulation.'[43] According to Moore, privacy is 'a right to control access to and uses of–places, bodies and personal information' and also as 'a right to maintain a certain level of control over the inner spheres of personal information and access to one's body, capacities and powers.'[44] Schoeman sees privacy as 'the measure of control an individual has over one's private matters'[45] and that, some have considered privacy as a claim, entitlement or right of an individual to determine what information about himself (or herself) may be communicated to others.[46] Belinger et al define the concept as the ability to manage information about oneself.[47]

Miller says privacy is 'the individual's ability to control the circulation of information relating to him.'[48] Parent defines it as 'the condition of not having undocumented personal knowledge

40 Irvin Altman, The Environment and Social Behaviour, Privacy, Personal Space, Territory and Crowding (Monterey Books, California, 1975) 1.
41 Lauren Henry Scholz, 'Information Privacy and Data Security' (2015) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2600495> accessed 11 April 2021.
42 Julie Cohen, 'What Privacy is for?' (2013) 126 Harvard Law Review, 2.
43 Anita Allen 'Privacy as Data Control; Conceptual Practical and Moral Limits of the Paradigm'(2000) 32 Connecticut Law Review, 861–835.
44 Adam Moore, 'Defining Privacy' (2008) 39(3) Journal of Social Philosophy, 411–428.
45 Ferdinand Schoeman, 'Privacy: Philosophical Dimension of the Literature' in Ferdinand D. Schoeman (ed) Philosophical Dimensions of Privacy: An Anthology. (Cambridge University Press, Cambridge, 1984) 1.
46 Schoeman (n 32).
47 France Belanger, Janine S. Hiller, and Wanda J. Smith, 'Trustworthiness in Electronic Commerce; The Role of Privacy, Security and Site Attributes' (2002) 11 Journal of Strategic Information Systems, 245–270.
48 Arthur Miller (n 6).

about one possessed by others.'[49] Marmor argues that privacy is grounded in 'interest in having a reasonable measure of control over the ways in which people can present themselves (and what is theirs) to others.'[50] Solove defines privacy as a 'fundamental right, essential for freedom, democracy, psychological wellbeing, individuality and creativity.'[51] Clarke describes it as the interest that individuals have in sustaining personal space free from interference by other people and organisations.[52]

Bevier describes privacy as a 'chameleaon-like' word used denotatively to designate a wide range of widely disparate interests–from confidentiality of personal information to reproductive autonomy and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name.'[53] Privacy has also been described in four senses: freedom to select seclusion, freedom to engage in undisturbed intimacy with a group of selected individuals, freedom to remain anonymous to others and freedom to remain protected by not revealing any personal information.[54]

In his account, Holvast describes privacy as 'a right to be let alone and a right of each individual to determine under ordinary circumstances, what his or her thoughts, sentiments and emotions shall be when in communication with others.'[55] Bok defined privacy as the 'condition of being protected from unwanted access by others–either physical access, personal information or attention'[56]

49 William A. Parent 'Privacy, Morality and the Laws' (1983) 12(4) Philosophy & Public Affairs, 269–288.
50 Andrei Marmor 'What is Right to Privacy' (2015) 43(1) Philosophy & Public Affairs, 3–26.
51 Daniel Solove, Understanding Privacy, Harvard University Press, Massachusetts, 2008) 5.
52 Roger Clarke, 'What's Privacy' http://www.rogerclarke.com/DV/Privacy.html accessed 1 April 2021.
53 Lillian Bevier, Information about Individuals in the Hands of Government: Some Reflections on Mechanism for Privacy Protection (1995) William & Mary Bill of Right Journal, 455.
54 Saed Alitajer & Ghazeleh Molani Nejoumi, 'Privacy at Home; Analysis of Behavioural Patterns in the Spatial Configuration of Traditional and Modern Houses in the City of Hamedan Based on the Notion of Space Syntax (2016) 5 frontiers of Architectural Research 341–352.
55 Jan Holvast 'History of Privacy' in Vashek Matyas, Simone Fisher–Hubner & Petr Svenda (eds) *The future of Identity in the Information Society*, (2008) IFP Advances in Information Communication Technology, 1.
56 Sissela Bok, Secrets on Ethics of Concealment and Revelation (Phantom books, New York, 1983).

Posner defined it as 'right to conceal discreditable facts about oneself,'[57] Inness says privacy is the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring or liking'[58] Lukacs notes that one of the attempts that best captured privacy is Szabo's definition as 'the right of the individual to decide about himself /herself'[59] and Gross sees privacy as the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited.[60] McCloskey on his own, briefly defines privacy as the 'control over when and by whom the various parts of us can be sensed by others.'[61]

Taking their cue from America and other parts of the world, a number of Nigerian authors have also defined privacy in many ways: Anozie refers to privacy as a situation in which the private sphere of the individual is respected in other words, accorded protection from judgemental or hypnotical public.'[62] Olomojobi views privacy as exclusion of the public eye from prying into any individual affairs, and the protection of image and ineffectual access to control one zones of exclusivity, space and confidential information.[63] Nwauche also notes that privacy is the right of the individual to be protected against intrusion into his personal life or affairs or those of his family by direct physical means or by publication of information[64] but this attempt however appears to have included private and family life in the definition. The Nigerian Supreme Court has also defined privacy as a right to

57 Richard Posner, The Economic of Justice (Harvard University Press, Massachusetts, 1981).
58 Julie Inness, *Privacy, Intimacy, and Isolation* (Oxford University Press, Oxford, 1992).
59 See Adrienn Lukacs, 'What is Privacy; The History and Definition of Privacy' (2016) University of Szeged, 16.
60 Hyman Gross, 'The Concept of Privacy (1967) 42(1) New York University Law Review, 30, 35–36.
61 See also H. J. McCloskey 'Privacy and the Right to Privacy' (1980) 55 (211) Cambridge University Press, Cambridge, 17, 23.
62 Miriam Chinyere Anozie, 'Abortion and Homosexuality Prohibitors Regimes Versus the Right to Privacy in Nigeria' (2020) 46 (3) Commonwealth Law Bulletin 483, 486.
63 Yinka Olomojobi, 'Right to Privacy' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062603> accessed 29 March 2021.
64 Enyinnna S. Nwauche 'The Right to Privacy in Nigeria (2007) 1 CALS Review of Nigerian Law and Practice, 64, 65.

protect ones thought, conscience or religious belief and practice from coercive and unjustified intrusion and one's body from unauthorised person.[65] Conclusively, while this book does not seek to suggest an all–encompassing definition or description of privacy, from an aggregation of the proceeding attempts, I safely view privacy as a fundamental right protection afforded a natural person from undesired or unauthorised interference with his/her personal affairs or relationships by whatever means irrespective of the purpose.

65 See Olumide Babalola, *Babalola's Law Dictionary* (2nd ed. Noetico Repertum, Lagos, 2019) 346: see also Medical Dental Practitioners Disciplinary Tribunal v Okonkwo (2001) LPELR 1856(SC).

CHAPTER TWO

Taxonomy and Typology of Privacy

The terms 'taxonomy' and 'typology' have been used interchangeably as classification methods.[66] The two classification concepts are however similar with the basic difference being, typology is conceptual and taxonomy empirical.[67] While Koops et al. prefer to write a typology of privacy, Solove did a taxonomy but both academic interventions were comprehensive enough to capture the respective authors' perspective and understanding of the classes, categories or components of privacy.[68] Notwithstanding the lack of consensus among scholars and researchers on definition of privacy, its classification or categorisation did not generate as much debate, hence, this chapter is devoted to a discussion of the identified inexhaustive classes or categories of privacy.

Privacy of the Person (bodily privacy) or personal privacy.

Clarke notes that this protects integrity of individuals body in relation to physiological and safety consciousness.[69] It guarantees

66 Roxane Borgès Da Silva, 'Taxonomy and Typology: Are they really synonymous?' (2014) 25(5) Santé Publique, 633–7.
67 Kenneth D. Bailey, Typologies and Taxonomies: An Introduction to Classification Techniques (Sage Publication, California, 1994) 6.
68 Bert–Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Skorvanek, Tomislav Chorkrevski and Masa Galic, 'A Typology of Privacy' (2017) 38 U.PAJ. Intl l, 483; Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154 (3) University of Pennsylvania Law Review, 477, 564.
69 Roger Clarke, 'What is Privacy' (2006) < http://www.rogerclarke.com/DV/Privacy.html> accessed 29 March 2021.

an individual, the inviolable right of his bodily features, characteristics and information from the prying eyes of others as a private affair of the subject.[70] Bodily privacy guarantees protection for physical selves against intrusive and invasive activities (e.g cavity searches, drug testing).[71] Personal privacy must however be distinguishable from 'confidentiality' which has to do with trust in another person with respect to private information management as opposed to personal privacy which relates to oneself.[72]

Privacy of personal behaviour and action.

Clarke described this as 'media privacy'[73] and it covers sanctity and respect for intimacy, sexual orientation and related activities, political engagements and religious beliefs and practices. Privacy in this context is not limited to private spaces but it extends to activities in the public.[74] The European Court of Human Rights (ECtHR) observed in *Hannover v. Germany* that 'there is a zone of interaction of a person and others, even in a public context, which may fall within the scope of private life.'[75]

Moreham notes that engaging in voluntary intimate activities in private of public does not necessity take away reasonable expectation of privacy.[76] In the determination of what behaviour or action falls under privacy protection, it has been observed that, such activities will be subjected to consideration of whether in respect of the disclosed facts, the person in question had

70 Rachel L. Finn, Michael Friedewald, and David Wright, 'Seven Types of Privacy' in Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet (eds) *European Data Protection: Coming of Age*, (Springer Publishing, New York, 2013) 1.
71 Global Internet Privacy Campaign, 'An International Survey of Privacy Laws and Practice' < http://gilc.org/privacy/survey/intro.html > accessed 2 April 2021.
72 Williams J. Winslade and Judith Wilson Ross, 'Privacy, Confidentiality, and Autonomy in Psychotherapy' (1985) 64(4) Nebraska Law Review, 580, 582.
73 Roger Clarke, 'Introduction to Dataveillance and Information Privacy and Definition of Terms' (1997) < http://www.rogerclarke.com/DV/Intro.html> accessed 28 March 2021.
74 Rache L. Finn et al (n 56) 1.
75 No. 317. 7 February 2012
76 See N.A. Moreham, 'Privacy in Public Places' (2006) 65(5) The Cambridge Law Journal, 606–635.

a reasonable expectation of privacy.'[77]Acquisti argues that, individual's behaviour which are often dictated by cultural or social patterns are privacy–sensitive and they could influence decision making activities of individuals.[78] Individuals' perceived behavioural patterns are now used to track them especially for marketing purposes with serious consequences on consumers' privacy.[79]

Privacy of personal communication

This has been stated to include 'interception privacy' i.e., 'the freedom that comes with choice to communicate with others devoid of fear of or actual interception or monitoring of such calls.'[80] Solove notes that, for a long time, individuals had been uncomfortable with audio surveillance and eavesdropping impact privacy.[81] This class of privacy seeks to guard against interception of all forms of communications and it is protected by relevant wiretapping legislation.[82] On the legal protection available for personal communication, Blackstone notes that 'eavesdroppers, or such as listening under walls or windows or the eaves of a house, to hearken after discourse and thereupon to frame slanderous and mischievous tales on a common nuisance and presentable at the court–leet'[83]

77 Lord Hoffnann in Campbell v MGN Ltd (2004) UKHL 22, (2004) 2 AC 457; See also Richard G. Wilkins, 'Defining the Reasonable Expectations of Privacy: An Emerging Tripatrite Analysis (1987) 5(5) Vanderbilt Law Review, 1079.
78 Alessandro Acquisti 'Privacy and Rationality in Individual Decision Making' IEEE Security Privacy 3(1) 26.
79 Lorrie Faith Cranor 'Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2013) 10 Journal on Telecommunications and High Technology Law, 10, 273–308.
80 Clarke (n 73).
81 Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154 (3) University of Pennsylvania Law Review, 477, 564. He also that, California prohibited interception of telegraph communities and the US Congress enacted the Federal Communications Act in 1934 to prohibit wiretapping.
82 Ferdinand J. Jr. Zeni, 'Wiretapping–The Right of Privacy versus the Public Interest' (1950) 40(4) Journal of Criminal Law and Criminology, 476.
83 Sir William Blackstone, Commentaries on laws of England (1769).

Informational (information) privacy.

This is also referred to as 'data privacy,' 'data protection,' or privacy of personal data and images.[84] Although many scholars are torn between the difference between the data privacy (US concept) and data protection (European concept) on one hand and their inter–relatively on the other hand, some writers resort to the adoption of data privacy in their works even when they intend data protection.[85] Data privacy is 'that aspect of privacy that safeguards data subjects' interests and rights which interests are usually privacy, personal autonomy and integrity–related.'[86] The interchangeable use of all these terms–data privacy, data protection, information privacy etc–within the context of privacy is foundation–sensitive.[87] Bygrave dismisses the divergence in terminologies as issues of form rather than substance especially since they practically refer to the same concept of privacy from different dimensional point of view.[88] To further confirm international recognition of the concept, even the ECOWAS Supplementary Act on data protection recognises 'privacy of data.'[89]

Information privacy is 'the claim of individuals groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others'[90] It

84 Blume says data protection translates to informational privacy. See Peter Blume 'Data Protection and Privacy–Basic Concepts in a Changing World' (2010) Scandinavian Studies in Law, 151.
85 The term data privacy has been adopted in many scholarly works. See Rachel Mulheron, 'A Potential Framework for Privacy. A Reply to Hello' (2006) 69 M.L.R. 679; Nataraj Venkataramanan, *Data Privacy Principles and Practice* (CRC Press, Florida, 2016); Vicenc Torra, *Data Privacy: Foundations, New Developments and the Big Data Challenge* (Springer Publishing, New York, 2017), Gerardus Blokdyk, *Data Privacy. A Complete Guide* (Create Space Independent Publishing Platform, California, 2018); Alex Makulilo (ed), *African Data Privacy Laws* (Springer Publishing, New York, 2016); and Nora Ni Loideain *EU Data Privacy Law and Serious Crime* (Oxford University Press, Oxford, 2020) etc.
86 See Lukman Adebisi Abdulrauf, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' (Published LLD thesis, University of Pretoria, 2015).
87 Ibid.
88 Lee Bygrave, Data Privacy Law: An International Perspective, (Oxford University Press, Oxford, 2014) 272.
89 Supplementary Act A/SA.1/01/10 on Personal Data Protection within the ECOWAS, 2010, article 2.
90 Alan Westin, *Privacy and Freedom* (New York Athenum, 1967) 48.

is the process of managing boundaries across different social contexts which boundaries may shift, collapse or re–emerge of social circumstances change.[91] The concept refers to a combination of communication privacy and data privacy and that, it guarantees individuals the right to ensure that their personal data are not accessed by others without restraint and where such exists, individuals must still retain control of the use of such personal data.[92] Belanger et al define informational privacy as the desire of individuals to control and have some influence over data about themselves.[93]

Finn et al observed that privacy of data and images guarantees personal autonomy and gives a feeling of self–empowerment.[94] Stone et al defined it as the capacity of individuals to control personally (vis a vis other individuals, groups, organisation etc) information about one's self.[95] In another account, Smith, Milberg and Burke further note that, the considerations and dimensions of information privacy are: collection, unauthorised secondary use (internal), unauthorised secondary use (external), improper access, errors, reduced judgement (issues around automated decision making), combining data (issues concerning data aggregation).[96] Informational privacy in this context, involves individual's apprehensions over monitoring of their communications, undesirable storage or disposal of their personal data, surveillance of any kind and an overall control their

91 Philip Fei Liu, Jessica Vitak and Michael T. Zimmer, 'A Contextual Approach to Information Privacy Research (2019) 4 Journal of the Association for Information Science and Technology, 1.
92 Clarke (n 69).
93 France Belanger and Robert Crossler, 'Privacy in Digital Age: A Review of Information Privacy Research in Information Systems' (2011) 35(4) MIS Quarterly, 1017–1041.
94 Finn (n 62).
95 Eugene Stone, Hal G. Guetal, Donald Gardner and Stephen McClure, 'A Field Experiment Comparing Information Privacy Values and Beliefs and Attitudes Across Several Types of Organisations' (1983) 68(3) Journal of Applied Psychology, 459–468.
96 Jeff Smith, Sandra J. Milberg and Sandra J. Burke, 'Information Privacy: Measuring Individual's Concerns About Organisational Practices' (1996) 20(2) MIS Quarterly, 167.

information in other's possession'[97] and Solove argues that this category is broader and with a wider spectrum than the American tort of privacy as conceived by Prosser.[98]

Conclusively, whether referred to as 'informational privacy', 'information privacy', 'data protection', 'privacy of personal data' or 'image or data privacy,' this category of privacy guarantees control over personal information and prevents unauthorised access, use or misappropriation of such information.

Privacy of personal experience, thoughts and feeling

This 'new' category was identified by Clarke in 2013, stating that human experienced as mediated by digital platforms and devices are now a place of privacy experience which can be influenced by screen–meditated interactions.[99] Koops et al note that while this class was not well articulated by Clarke, it is interfered with, when individuals' visuals and readings are monitored.[100] The category guarantees the right to disclose or withhold thoughts and feelings and this is distinguishable from privacy of the person in the same manner the mind is distinguishable from the body.[101]

Physical privacy.

This is similar to the privacy of the person in the sense that, it relates to unauthorised or undesirable access to one's physical self. Moreham notes that the influence contemplated here is 'sensory' where privacy is violated by unauthorised entity listening on, or otherwise interfering with the victim's physique against his

97 Beate Rossler, The Three Dimensions of Privacy' in Bart van der Sloot and Aviva de Groot (eds) *The Handbook of Privacy Studies*, (Amsterdam University Press, Amsterdam, 2018).
98 Daniel J. Solove, *Understanding Privacy* (Harvard University Press, Massachusetts, 2008).
99 Clarke (n 55).
100 Koops (n 68).
101 Finn (n 62).

wish.[102] It is worthy of note that, physical privacy may however overlap with other classes of privacy.[103]

Associational privacy.

This class was identified by Allen in her account of the types of privacy protected at Common law.[104] Koops et al conclude that this class is complex in that, it relates to groups and their internal workings entitling the members' right to keep their membership details and information private.[105] Kalhan, in an analysis of the *NACCP v Alabama* case[106] with respect to information privacy somewhat 'created' the category by arguing that, compulsion to disclose immigration status may expose data subjects to discrimination and an individual's desire to keeping such information private is tantamount to 'associational privacy.'[107]

Allen added that, enforcement and enjoyment of associational privacy will preclude government agencies from compelling even a controversial group from identifying its members in deserving cases where such members do not want to be so identified.[108] The class guarantees freedom to connect, relate and associate with others without being monitored or compelled to disclose such relationships.[109]

Racial Privacy. By arguing that 'racial information' is not sufficiently protected under informational privacy, Allen carved

102 N.A Moreham, 'Beyond Information; Physical Privacy in English Law' (2014)73(2) The Cambridge Law Journal, 359.
103 Moreham, (n 90)
104 Anita Allen, Unpopular Privacy: What We Must Hide (Oxford University Press, Oxford, 2011) 259.
105 Koops et al (n. 68).
106 NAACP v. Alabama, 357 U.S. 449 (1958)
107 Anil Kalhan, 'The Fourth Amendment and Privacy: Implications of Interior Immigration Enforcement' (2008) U.C. Davis Law Review, 113 217.
108 Anita Allen, 'Associational Privacy and the First Amendment: NAACP v Alabama, Privacy and Data Protection' (2011) 1 Alabama Civil Rights & Civil Liberties Law Review, 13.
109 Koops (n 68).

out this category of privacy which not only seeks to recognise race as a sensitive data but to also reinforce the right of persons, of all races to privately co–exist.[110] This type of privacy often overlaps with freedom from racial discrimination and advocacy against public 'indiscriminate collection of information about individuals' races for undisclosed future use.[111]

Intellectual privacy. Richard originated this category and described it as a right that 'safeguards the integrity of our intellectual activities by shielding them from the unwanted gaze or interference of others.'[112] With the breakthroughs in technology, intellectual surveillance is now seamless and more frequent than ever and this right offers protection for an individual's records of intellectual engagements.[113] Richard contends that, this type of privacy does not seek to remedy tortious injuries but coordinates public discourse and thought process and how it ultimately relates to freedom of speech. [114]

Cohen observed that apart from the conventional notion of privacy, especially in the American constitution, the First amendment had introduced the 'right of intellectual privacy' and he argued that the general principle of law recognised that the freedoms of expression and association would be violated if an individual is compelled to reveal the contents of his intellectual life.[115] This, he notes disapproves invasion and inquiry into a person's library to reveal the kind of books or literary materials he reads. These kinds of invasion of privacy were prominent during the pornography cases.[116]

110 Anita Allen, 'Race, Face and Rawls' (2004) 72 Fordham Law Review, 1677–1696.
111 See Lior Strahilevitz, 'Privacy Versus Anti–discrimination' (2008) 75 University of Chicago Law Review, 363.
112 Neil Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (Oxford University Press, Oxford, 2017).
113 Ibid.
114 Neil Richards, 'Intellectual Privacy' (2008) 87 Texas Law Review, 387.
115 Julie E. Cohen, 'Intellectual Privacy and Censorship of the Interest' (1998) 8 Seton Hall Const. L.J. 693.
116 See Stanley v Georgia 394 U.S. 557 (1969) where the US Supreme Court established the right to privacy in mere possession of obscene materials.

Decisional Privacy.

This class relates to an individual's personal decisions and preference in life. The framework for decisional privacy has been posited to have been developed by the decision in *Roe v Wade*[117] where the US Supreme Court affirmed a pregnant woman's right to have an abortion without government's interference.[118] Floridi defines decisional privacy as the right to determine one's own cause of actions.[119] Margulis notes that this right relates to the freedom an individual exercises in making a personal decision on when and how to talk in private or public as he considers proper in every given circumstance.[120]

This class of right is activated in cases concerning abortion, birth control, and sexual preferences etc.[121] It is broadly defined as the right against unwanted interference to individual's actions and decisions.[122]The interference in this context, may appear in the form of unauthorised or undesired access to one's private activities, behavioural habits, plans and decisions by known and/or unknown natural or artificial entities which influence, change, comments on or otherwise meddles without a reasonable expectation of such interference.[123]

Decisional privacy is all about an individual's liberty to make weighty personal decisions without interference, hence, it is 'self–defining,' 'choice–based' and ultimately contemplates the right to make personal decisions without government or other

117 410 U.S. 113.
118 Bart van der Sloot 'Decisional Privacy 2.0: The Procedural Requirements Implicit in Article 8 ECHR and its Patents Impact on Profiling' (2017) 7(3) IDPL 190–201.
119 Luciano Floridi, *The Ethics of Information* (OUP Oxford, 2013) 257.
120 Stephen Margulis, 'Privacy as Social Law and Behaviour Concept' (2003) 59(2) J. Soc. 244.
121 Anita Allen. 'Taking Liberties: Privacy, Private Choice and Social Contract Theory' (1998) 56 UC in L Rev 411, 466.
122 Beate Rossler, *The Value of Privacy* (1st edn. Polity Press, Cambridge, 2005).
123 Marjolein Lanzing, 'Strongly Recommended' Revisiting Decisional Privacy to Judge Hyper–nudging in Self Tracking Technologies' (2019) 32 Philosophy Technology, 549–568.

entities' interference.[124]

Proprietary and Reputational Privacy

Koops et al explain that this class relates to an individual's reputation i.e 'right to one's honour' as found in most Countries' constitutions.[125] The Universal Declaration of Human Rights (UDHR) and International Convention on Civil and Political Rights (ICCPR) both guarantee reputational privacy by the inclusion of 'honour and reputation' in their texts.[126] It has been noted that, the American Convention on Human Rights also protects reputational privacy by prohibition wanton interference with individual's reputation and provides succour where such rights are threatened. In the case of *Pfeifer v Austria,*[127] the ECtHR gave credence to reputational privacy when it ruled on the equivalence of reputation with right to freedom of expression under European law. On the European courts' attitude towards reputational privacy, Smet notes that, the court has alluded in a number of cases that: "the right to protection of one's reputation is . . . one of the rights guaranteed by (Article 8) as one element of the right to respect for private life.'[128]

Privacy of thoughts and feelings

Finn et al identified this category which rather than focus on individual's physical body, protects the transitory activities in such individual's mind.[129] This class guarantees the right of choice to show or otherwise keep private one's thoughts and feelings.

124 Roger J.R. Levesque, *Adolescence, Privacy and the Laws: A Developmental Science Perspective*, (Oxford Scholarship Online, 2016).
125 Koops et al (n 64).
126 Elizabeth Anne Kirley, Reputational Privacy and the Internet: A Matter for Law? (2015) published PhD thesis Osgoode Hall Law School, York University, 2015.
127 Nos. 33677/10 and 52340/10.
128 Stijn Smet, 'Freedom of Expression and the Right to Reputation: Human Rights in Conflict' (2010) 26 Am. U. Int'l Rev., 183, 184.
129 Finn (n 62).

Although one's thoughts and emotion are not easily accessible without the individuals overt act of revealing them, individuals reserve the freedom of keeping them private from the prying eyes of known and/or unknown entities.[130]

It is observed that, with the current technological advancement, physiological biometrics can now interfere with thoughts and feelings by processing intimate patterns and other sensitive information which can be used to arrive at conclusions on suspicion or likelihood of certain end results.[131]

Instructively, Warren and Brandies alluded to this class of privacy in persuasive terms that, 'if then, the decisions indicate a general right to privacy for thoughts, emotions, sensations, these should receive the same protection, whether expressed in writing or in the conduct in conversation, in attitudes or in facial expression.'[132] Stark however notes that emotions are highly significant in the context of privacy with the example of digital mediation of emotions enabled by some sort of surveillance of users' emotional life.[133]

Relational privacy

This is a variant of informational privacy which relates to an individual's right to control the transmission of personal information within the context of a closed group and within the sphere of social interactions.[134] Some proponents of this class argue that right to privacy can only truly be exercised within a

130 David Best, 'Mind, Act and Philosophy' (1986) 20(3) The Journal of Aesthetic Education, 16, 17.
131 See Finn et al (n 100).
132 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review, 11.
133 Luke Stark, 'The Emotional Context of Information Privacy' (2016) 32(1) The Information Society, 16; Andrew Mcstay, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) Big Data & Society 1–12.
134 Robert H. Sloan and Richard Warner, 'Relational Privacy: Surveillance, Common Knowledge and Coordination' (2017) 11(1) University of St. Thomas Journal of Law and public Policy, 7.

dense of relationships.'[135]

Relational privacy shifts focus from self to interrogations on how networked relationships enhance or otherwise impact self–autonomy within the context of a group interactions rather than individual exclusion.[136]

In exercising relational privacy, individuals engaging in group interactions are still presumed to have reasonable expectations of privacy within such webbed–relationships.[137] In his account on relational privacy, Sacharoff notes that, the courts often ignore this category of privacy by treating the concept as "all or nothing" i.e where privacy is conceded or waived in favour of one person, then it has been ceded to every one within the space.[138] He further notes that the government has been erroneously categorized by the courts as member of the public without taking cognizance of the regular situations where citizens are allergic to the government's prying eyes.[139]

This class was enforced in a recent English case of *JQL v NTP*[140] where the UK High Court awarded damages against an uncle for posting information about the niece's earlier treatment for mental health and self–harm in the family's closed Facebook group page. The court held that the niece has reasonable expectation of privacy over personal information even within the context of her family interactions.

135 Stuart Hargreaves, 'Relation Privacy and Tort' (2017) 23 (3) William and Mary Journal of Women & the Law, 433.
136 See Sara Bannerman, 'Relational Privacy and the Networked Governance of the Self? (2019) 22(14) Information, Communication and Society 2187–2202.
137 Joel R. Reidenberg, 'Privacy in Public (2014) 69 Univeristy of Miami Law Review 141.
138 Laurent Sacharoff, 'The Relational Nature of Privacy' (2013) 16(4) Lewis & Clark Law Review 1249.
139 Sacharoff (n 183): See also Jose Roberto Goldim and Sahra Gibbon 'Between Personal and Relational Privacy: Understanding the Work of Informed Consent in Cancer Genetics in Brazil' (2015) 6(3) Journal of Community Genetics, 287–293; J Lyn Entrikin, 'Family Secrets and Relational Privacy' (2020) 74 (3) University of Miami Law Review 781–887: Marilyn Friedman, 'Relational Autonomy and individual' (2013) 63(2) The University of Toronto Law Journal, 327–341.
140 (2020) EWHC 1344 (QB).

Locational or spatial privacy.

This relates to the claims of individuals to determine for themselves when, how and to what extent, locational information about them is communicated with others.[141] The crux of this class of privacy is the control and safeguard of location information which has been defined as 'any data which places one at a particular location at any given point in time or at a series of location over time.'[142] Such locational information can be utilised for the monitoring and surveillance in the course of compiling records of an individual's movements in public space[143] and that CCTV, Wi–Fi Tracking System, facial recognition devices interfere with locational and spatial privacy.

Physical or accessibility privacy

This is the freedom enjoyed by an individual from sensory interreference which is exercisable by restricting others from having bodily interactions with the individual or invasion of his personal space[144] and its origin is traceable to Warren and Brandeis' "right to be let alone" or being 'free from intrusion.'[145]

Psychological privacy. This also refers to mental privacy. It is the right of an individual to limit or restrict others' capacity to access and/or influence his inner thoughts or mind.[146] Mental

141 Matt Duckham and Lars Kulik, 'Location Privacy and Location Aware Computing' <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.366.1455&rep=rep1&type=pdf> accessed 29 March 2021.
142 Teresa Scassa, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy' (2010) 7(1) Canadian Journal of Law and Technology, 44.
143 Anne Uteck, 'Ubiquitous Computing and Spatial Privacy' in Ian Kerr, Valerie Steeves and Carole Lucock (eds) *Lessons from the Identity Trial: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, Oxford, 2009) 83–102.
144 Luciano Floridi, Fourth Revolution (Oxford University Press, Oxford, 2014) 272.
145 Herman Tavani, 'Informational Privacy Concepts Theories and Controversies' in Kenneth Himma and Herman T. Tavani, (eds) *The Handbook of Information and Computer Ethics* (John Wiley & Sons, New Jersey, 2008) 131.
146 Herman Tavani, 'Information Privacy: Concepts, Theories and Controversies' in Kenneth Einar Himma and Herman T. Tavani (eds) *The Handbook of Information and Computer Ethics* (John Wiley & Sons, New Jersey, 2008).

privacy concerns freedom from psychological interference or intrusion also achieved through restriction of others.[147]

Sexual privacy

This class relates to 'social norms governing the management of boundaries around an individual's intimate life.' It regulates the ramification of other's access to information and details about one's nudity, sexual thoughts, desires, fantasies, intimate activities, sexual communications, and orientation.[148] In her account, Allen particularly demonstrates the dynamics of sexual privacy to women and the LGBTQ Community, and further views sexual harassment in the workplace as some invasion of sexual privacy.[149]

Active privacy

Al-Fedaghi defines this type of privacy as the active freedom of an individual when dealing with his private information, to claim the right to control the extendability of others' involvement in these private affairs without intereference.'[150]

Passive privacy

This is a notion of privacy where an individual is a passive agent in dealing with his personal information, hence he/she does not have active control but he/she enjoys freedom from other's

147 Floridi (n 128).
148 For a comprehensive account on sexual privacy, see Danielle Keats Citron, 'Sexual Privacy' (2019) 128(7) The Yale Law Journal, 1879.
149 See Anita Allen, 'Privacy Torts: Unreliable Remedies for LGBT Plaintiffs' (2010) 98 California Law Review 1711–1721); see also Moira Arkenhead, 'A Reasonable Expectation of Sexual Privacy in Digital Age' (2018) 41 Dalhousie L.J 273.
150 Sabah Al–Fedaghi, 'The Right to be let Alone and Private Information' in Chin–Sheng Chen, Joaquim Filipe, Isabel Seruca and José Cordeiro, (eds) *Enterprise Information Systems VII* (Springer International Publishing, New York, 2007).

interference by being let alone.'[151]

Post–mortem privacy

Buitelaar defines this as the 'right of a person to preserve and control what becomes of his reputation and dignity after death.'[152] This category is posited to protect the secrets or memories of individuals after death.[153]

Going through the foregoing categorisation of privacy, it is observed that, the typology and taxonomy are not only subjective to the proponents, they sometimes overlap in their exercise and application. Hence, it is worthy of reiteration that, the categories of privacy are neither closed nor cast in stone.

151 Al–Fedaghi (n 150).
152 J.C Buitelaar, 'Post–Mortem Privacy and Informational Self–Determination' (2017) 19 Ethics Information Technology, 129–162.
153 Lilian Edward and Edina Harbinja, Protecting Post–Mortem Privacy: Reconsidering the Privacy interest of the Deceased in Digital World; (2013) 32(1) Cardozo Arts & Entertainment Law Journal, 101–147; see also Edina Harbinja, 'Post–Mortem Privacy 2.0: Theory, Law, and Technology' (2017) 31(1) International Review of Law, Computers & Technology, 26–42.

CHAPTER THREE

Right to Privacy in Nigeria

The african continent did not place as much value on privacy as it did in the last two decades. Some researchers even doubted whether the concept exists on the continent while others question its appreciation within the African communal Internet of Things (IOT).[154] Makulilo however refers to the claims as 'overstated and lacking empirical evidence' while agreeing that discussion on privacy had been dominated by western commentators until very recently. He also agrees that claims for individualism, self–autonomy and related notions are manifesting in African societies.[155]

The premium placed on privacy by the African continent is further interrogated when it is considered that, the most prominent international instrument on human rights in Africa–the African Charter on Human and Peoples Right (African Charter) does not have a provision on privacy. The Charter was adopted in 1998–fifty years after the adoption of the Universal Declaration on Human Rights yet, right to privacy was conspicuously omitted from the instrument. Some Nigerian academics have however

154 Lee Bygrave, 'Privacy Protection in a Global Context–A Comparative Overview' (2004) 47 Scandinavian Studies in Law 319–348 at p. 328; David Banisar, 'Privacy and Data Protection' Around the World' (1999) Conference Proceedings of 21st International Conference on Privacy and Personal Data Protection Hong Kong; Hanno Olinger, Johannes Britz & Marton Olivier 'Wester Privacy and/or Ubuntu? Some Critical Comments or the influence in the forthcoming Data Privacy Bill in South Africa (2007) 39 (1) International information & Library Review, 31.

155 Alex Makulilo, 'A Person is a Person Through Other Persons'–Critical Analysis of Privacy and Culture in Africa' (2016) 7 Beijing Law Review 192–204.

suggested that the omission was for the purpose of promoting the characteristic communalism of African societies[156]–a claim that is not manifestly supported in theory or reality.

In 1954, when the enactment of the Nigeria (Constitution) Order in Council 1954 Lyttleton Constitution) effectively made the country a federation, a provision on right to privacy was inserted in the sixth schedule marking its first notable entry into the Nigerian legal system.[157] However, Nigeria's discourse (as a republic) on privacy commenced upon its independence in 1960 when the (albeit imposed) Bills of Rights in the 1960 Independence Constitution made express provision for the fundamental right to private and family life which predominantly guaranteed citizens' entitlement to respect for their private and family life, his home and correspondences.[158] Proehl alluded that, the notion of self–autonomy introduced by the new (1960) Constitution was imported as a foreign concept in the following terms:

"[i]t is fair to say that, by and large, the individual Nigerian living under the 1960 Constitution, while not able to boast that he enjoyed Holmes' "right to be let alone'–since neither communal life in the bush nor life in Nigeria's crowded urban centres permits upon than many of his African brethren."[159]

However, in the build–up to the 1960 Constitution, Nigerian societies were predominantly governed by beliefs that socio–

156 See Yinka Olomojobi 'Right to Privacy in Nigeria (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062603> accessed 30 March 2021; Akin Ibidapo–Obe, Essays on Human Rights Law in Africa (Concept Publications Ltd, Lagos, 2005); Osita Ogbu, Human Right Law and Practice, (2nd edn, Snaap Press, Enugu, 2013) 280–281.

157 See Paul O. Proehl, 'Fundamental Rights Under the Nigerian Constitution, 1960–1965' (1970) 8 Occasional Paper, African Studies Centre, University of California, 32. See also Alhaji Umar Alkali, Abbo Jimeta, Awwal Ilyas Magashi and Tijjani Musa Buba, 'Nature and Sources of Nigerian Legal System: An Exorcism of a Wrong Notion' (2014) 5(4) International Journal of Business, Economics and Law, 1.

158 Constitution of the Federation of Nigeria 1960, section 22 (1) provides that: "Every person shall be entitled to respect for his private and family life, his home and his correspondence."

159 See Paul O. Proehl, 'Fundamental Rights Under the Nigerian Constitution, 1960–1965' (1970) 8 Occasional Paper, African Studies Centre, University of California, 6.

political uprightness and 'good neighbourliness' could only be achieved with communal co–existence, thereby relegating the concept of self–autonomy and privacy to the background, even though it ultimately surfaced in the constitution.[160]

The first recorded attempt at litigating right to privacy in our country was the decision in *Olawoyin J.S. v Attorney General, Northern Region*[161] where the appellant–father of a juvenile–approached the court seeking to nullify a provision of the Children and Young Persons Law prohibiting the co–opting or participation of juveniles in politics, on the ground that it, interfered with the appellant's right to private and family life. Unfortunately, when the appeal got to the Supreme Court, the issue on private and family life was not addressed by the apex court as the appellant was adjudged lacking locus standi to sue for an alleged infraction of his child's fundamental right.[162]

Successive Nigerian Constitutions have retained the provision on privacy in varying terms: the 1963 version provided for the "respect for private and family life, home and correspondence'[163] but apart from the difference in the systems of government adopted, the 1960 and 1963 constitutions were substantially identical.[164] Like its predecessors, the 1979 Constitution also guaranteed the privacy of citizens, their homes correspondences, telephone conversations and telegraphic communications[165] and the provision had the effect of prohibiting public authorities from monitoring or surveiling citizens' private communications among

160 Babatunde Agiri, 'The Concept and Practice of Individual Rights in Nigeria 1950–1966: How Relevant is the American Constitutional Experience' (1991) 29(2) American Studies International, 55–68.
161 (1962) 1 ANLR 324 at 327.
162 It is however worthy of note that, the requirement for locus standi in fundamental rights cases has now been jettisoned in favour of freer access to justice and public interest litigations. See Olumide Babalola v Attorney General of the Federation (2018) LPELR–43808 (CA).
163 Constitution of the Federation of Nigeria, 1963, section 23(1).
164 Michael P. Sang, 'Democracy in Nigeria' (1958) 9 (2) National Black Law Journal, 129.
165 Constitution of the Federal Republic of Nigeria 1979, section 34(1).

other personal activities.[166] The third republican Constitution of 1989 also provided for right to privacy in the following terms: 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed' but in the marginal notes, this was described as 'right to private life' as opposed to private and family life which existed in the previous constitutions.

The phrase "private and family life" was likely copied from article 8 of the European Convention on Human Rights which was adopted in 1948–twelve years before Nigeria's first republican Constitution was drafted in 1960,[167] however, the current 1999 Constitution mirrors the 1979 Constitution's provision on right to privacy verbatim.[168]

166 Moses E. Akpan, 'The 1979 Nigerian Constitution and Human Rights' (1980) 2(2) Universal Human Rights, 23.
167 See Muhammed Isah Shehu and Sirajo Ado Jahun, 'Constitutions Making, Amendments, Reviews and Nigeria's Political Development: The Political Economy and Unending Search' (2018) < https://www.academia.edu/36504422/Constitutions_Making_Amendments_Reviews_and_Nigeria_s_Political_Development_The_Political_Economy_and_Un_ending_Search> accessed 30 March 2021.
168 This is comprehensively discussed in chapter five.

CHAPTER FOUR

Privacy as a Tort

Privacy as we know it today, reportedly originated from the United States as a tort when two lawyers–Samuel Warren and Louis Brandeis (who later became a Judge) argued for the protection of individuals from invasion of privacy since it lacked legal backing in 1890 when they advocated for the remedy of an action in tort for damages.[169] These first proponents of privacy did not fragmentised the concept, rather they sought a coherent cause of action in the 'right to be let alone' using examples that depicted misappropriation of personal information and use or transmission of same in undesired manner.[170]

On the heels of the 1980 article which Harry Kulven Jr described as "the most influential law review of all,"[171] the New York Court of Appeal declined to recognise a cause of action in invasion of privacy but advised that, such cause of action could be easier recognised in the absence of precedent where a legislation exists on same[172] and consequently in 1903, the New York State enacted a law effectively recognising a cause of action for invasion of privacy[173] marking the beginning of the legislative journey of

169 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review, 193.
170 Lior Jacob Strahilevitz 'Reunifying Privacy Law' (2010) 98(6) California Law Review, 2007–2048.
171 Harry Kulven Jr., 'Privacy in Tort Law–Were Warren and Brandeis Wrong' (1966) 31 Law and Contemporary Problems, 326–341.
172 Roberson v Rochester Folding Box Co. 64 N.E 442 N.Y. 1902.
173 N.Y. Civ. Rights Law 50–51.

privacy as a statutory tort in the United States.[174]

However, seventy years after Warren and Brandeis' proposition of privacy that was critiqued for lacking 'order a legitimacy, [175] Prosser gave it some conceptual coherence by identifying four constituents of privacy. [176] In his theory that aided the development of concept of privacy in America at that time,[177] Prosser posited that privacy consists of four torts bound as one by their common name to wit: (a) intrusion into seclusion, solitude, or private affairs; (b) public disclosure of embarrassing private information; (c) publicity which places one in false light in the eye of the public; and (d) appropriation of one's name for another's advantage.[178] Ultimately, while Prosser's taxonomy redressed the privacy injuries of that time, it may not be sufficient to provide reprieve in this era of unprecedented technological advancement and seamless privacy intrusion.[179]

Tort of Privacy under English Law

The English courts have repeatedly expressed their unwillingness to create a tort of invasion of privacy. They have been emphatic in a number of cases that there exists no stand–alone general right to privacy, but the interest may be protected under existing causes of action and equitable remedies like breach of confidence,[180] malicious falsehood,[181] harassment,[182] trespass, defamation,

174 Daniel J. Solove 'A Brief History of Information Privacy Law' in Kristen J. Mathews *Proskaver on Privacy:A Guide to Privacy and Data Security Law in the Information Age* (PLI Press, New York, 2006).
175 Despite Prosser's claim that the 1890 article lacked legitimacy, it was conceded that the article impacted the law of privacy when courts began to award damages for invasion of privacy in subsequent cases until the trend was reversed in 1899. See Neil M. Richard and Daniel J. Solove, Prosser's Privacy Law: A Mixed Legacy' (2010) 98(6) California Law Review, 1887–1924.
176 See William L. Prosser, 'Privacy' (1960) 48(3) California Law Review, 385.
177 Neil Richards and Daniel J. Solove, 'Prosser's Privacy Theory: A Mixed Legacy' (2010) 98(6) California Law Review, 1887.
178 Prosser (n 138).
179 Daniel Keats Citron, 'Mainstreaming Privacy Torts' (2010) 96(6) California Law Review, 1805–1852.
180 Campbell v MGN Ltd [2003] QB 633.
181 Kaye v Robertson [1991] FSR 62.
182 Hunter v Canary Wharf Ltd [1997] AC 655.

nuisance[183] and infliction of personal or emotional harm, etc.[184]

The House of Lords in *Wainwright v Home Office* insistently reiterated the courts' stance on non–existence of common law or statutory right to privacy when Lord Hoffman extensively expressed the view that:

> *"My Lords, let us first consider the proposed tort of invasion of privacy. Since the famous article by Warren and Brandeis, the question of whether such a tort exists, or should exist, has been much debated in common law jurisdictions. Dean Prosser's taxonomy divided the subject into (1) intrusion upon the plaintiff's physical solitude or seclusion (including unlawful searches, telephone tapping, long–distance photography, and telephone harassment) (2) public disclosure of private facts and (3) publicity putting the plaintiff in a false light and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness. These, he said, at page 814, had different elements and were subject to different defences. The need in the United States to break down the concept of "invasion of privacy" into a number of loosely linked torts must cast doubt upon the value of any high–level generalisation which can perform a useful function in enabling one to deduce the rule to be applied in a concrete case. English law has so far been unwilling, perhaps unable, to formulate any such high–level principle.*

183 Khorasandjian v Bush [1993] QB 727.
184 Basil Markesinis, Colm O'Cinneide, Jörg Fedtke and Myriam Hunter–Henin, 'Concerns and Ideas about the Developing English Law of Privacy (And How Knowledge of Foreign Law Might Be of Help)' (2004) 52(1) The American Journal of Comparative Law, 133–208.

> *There are a number of common law and statutory remedies of which it may be said that one at least of the underlying value they protect is a right of privacy… But there are gaps; cases in which the courts have considered that an invasion of privacy deserves a remedy which the existing law does not offer. Sometimes the perceived gap can be filled by judicious development of an existing principle. The creation of a general tort will, as Buxton LJ pointed out in the Court of Appeal, at [2002] QB 1334, 1360, para 92, pre–empt the controversial question of the extent, if any, to which the Convention requires the state to provide remedies for invasions of privacy by persons who are not public authorities. For these reasons I would reject the invitation to declare that since at the latest 1950 there has been a previously unknown tort of invasion of privacy."*[185]

The English courts have variously observed that the remedies ordinarily sought under invasion of privacy could be accommodated under some existing common law torts and statutes like the UK Human Rights Act, Data Protection Act, etc and in the decision in *Campbell v Mirror Group Newspapers Ltd*,[186] the House of Lords extended the cause of action founded on breach of confidence to compensate for unauthorised publication of private information. In that case, Lord Nicholls noted that:

"In this country, unlike the United States of America, there is no over–arching cause of action for 'invasion of privacy.' But protection of various aspects of privacy is a fast–developing area of the law…." The common law or more precisely, courts of

185 (2003) UKHL 53.
186 Paula Goliker 'A Common Law Tort of Privacy? The Challenges of Developing a Human Rights Tort' (2015) 27 Singapore Academy of Law Journal, 711–788.

equity have long afforded protection to the wrongful use of private information by means of cause of action which became known as breach of confidence"[187]

The English Court of Appeal also observed in the decisions in *OBG Ltd v Allan*[188] and *Douglas v Hello*[189] that, 'as the law has developed breach of confidence, or misuse of confidential information now covers two distinct causes of action, protecting two different interests: privacy and secrets (confidential)'[190] but the English courts were hesitant to create or recognise a distinct tort of privacy for two reasons: one, the components of the cause of action in privacy are already captured in common law tortious actions malicious falsehood like trespass to person, nuisance, defamation, and as well as the equitable remedy in breach of confidence and secondly, causes of action seeking to prohibit publication of private information were seen as anti–free speech contrary to bills of rights guaranteeing freedom of expression.[191]

Conclusively, while it is conceded that, there exists no common law tort of invasion of privacy, such interests can now be sufficiently accommodated under various causes of action including the UK Human Rights Act, 1998, Data Protection Act, 2018 etc[192]

Tort of Privacy in Nigeria

Nigeria inherited the English Common law but since there was no

187 (2005) UKHL 61.
188 [2005] QB 762.
189 [2006] QB 125.
190 UK Parliament, 'Judgments–OBG Limited and others (Appellants) v. Allan and others (Respondents) Douglas and another and others (Appellants) v. Hello! Limited and others (Respondents) Mainstream Properties Limited (Appellants) v. Young and others and another (Respondents)' <https://publications.parliament.uk/pa/ld200607/ldjudgmt/jd070502/obg–8.htm#:~:text=As%20the%20law%20has%20developed,to%20keep%20these%20two%20distinct.> accessed 4 April 2021.
191 Samuel Beswick and William Fotherby, 'The Divergent paths of Commonwealth Privacy Torts' (2018) 84(2d) Supreme Court Law Review, 225–267.
192 Gavin Phillipson, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under Human Rights Act? (2003) 66(5) The Modern Law Review, 726–758.

common law or statutory tort of invasion of privacy to be inherited, unlike other torts which we inherited upon independence, Nigeria's tort of invasion of privacy does not owe its origins to the English law.[193] Although, some of the statutes enacted by the Nigerian parliament at the time were substantial reproduction of the English statutes including the Law Reform (Torts) Law,[194] it remains unclear how the provision on invasion of privacy was introduced into the Nigerian legislation when no such existed in the English statutes.[195]

From its long title, it would be seen that the Law Reform (Torts) Law which was Nigeria's first law on invasion of privacy was enacted to amend the previous law on contributory negligence as found in the English Law Reform (Contributory Negligence) Act 1945.[196] This law effectively created the statutory tort of invasion of privacy as proposed in Prosser's theory by prohibiting: (i) intrusion into others' private affairs; (ii) appropriation of others name for self–benefit and (iii) unauthorised publication of others private information.[197]

It is instructive to note that, invasion of privacy is currently a recognised tort in Lagos State.[198]

193 Oluwole Aluko and Gilbert Kodilinye, *The Nigerian Law of Torts* (Spectrum Books, Ibadan, 2001).
194 Cap 32, Laws of Western Nigeria.
195 The English Law Reform (Contributory Negligence) Act 1945 which was partly imitated by the Nigerian Law Reform (Torts) Law does not have any provision on invasion of privacy.
196 Enacted by the parliament of Western Region of Nigeria but later re–enacted by the Law Reform (Torts) Law, 2003.
197 Law Reform (Torts) Law, Laws of Western Region of Nigeria, 1959, section 3.
198 Sections 29 and 30 of the Law Reform (Torts) Law 2015 provide for the tort of invasion of privacy and remedies.

CHAPTER FIVE

Privacy as a fundamental right

FROM THE VARIOUS historical accounts, whether tied to Fitzjames Stephen's or Warren and Brandeis,' the consensus remains that privacy originated as a tortuous claim. Seventeen years before Warren & Brandeis' famous article that revolutionized the world's perception of privacy as a cause of action, Stephen had discussed the concept of privacy in terms of its intimacy to life and the expediency of observance of its sanctity by individuals and all other persons[199] and over 130 countries have subsequently made provisions for privacy as a fundamental right in their constitutions.[200]

In the US, privacy was first recognized as a constitutional right in the 1965 case of *Grisworld v Connecticut*[201] where the US Supreme Court affirmed the right of married couples to use birth control devices without government interference in that, the court nullified a law prohibiting the use of contraceptives on the ground that, is interfered with right to privacy in relation to intimate activities.[202] Privacy in the United Kingdom sprung up from the 1998 Human Rights Act (HRA) which transposed the Country's international obligation under the European Convention on Human Rights

199 James Fitzjames Stephen, Liberty, Equity Fraternity (Smith, Elder & Co., London, 1873). See also H.J. McCloskey 'Privacy and the Right to Privacy' (1980) 55 (211) Cambridge University Press, Cambridge, 17–38.
200 Refat Al–Sohan, 'Why Should Right to Privacy Be a Human Right?' < https://www.researchgate.net/publication/328725112_Why_Should_Right_To_Privacy_Be_A_Human_Right> accessed 11 April 2021.
201 381 U.S. 479 (1965).
202 For further reading, see Lackland H. Bloom, Jr 'The Legacy of Griswold' (1989) 511 Ohio Northern University Law Review, 511.

(the convention).[203] Prior to the passage of the HRA, the English parliament had declined a number of requests for the creation of a statutory right of privacy on many grounds.[204] The enactment of the HRA makes it possible for Britons to enforce right to privacy as provided under article 8 of the convention in the domestic courts thereby dispensing with the need for the UK parliament to create a stand–alone tort of privacy[205] especially since section 6 HRA enjoins the English courts to give effect to privacy right guaranteed under the convention.[206]

Before privacy was accepted by countries as a fundamental right, it gained international recognition in 1948 when the Universal Declaration of Human Right (UDHR) [207] became the first international document[208] that recognized the fundamental right to privacy guaranteeing protection against basic privacy issues like searches and seizure, and unwanted interference and other intrusive activities.[209]In spite of it non–binding nature, the UDHR has been described as 'common conscience for humanity'[210] representing itself as a 'common standard of achievement for all peoples and all nations' hence it has become the performance indicators for countries as far as respect for citizens' fundamental rights are concerned.[211] In guaranteeing right to privacy, the UDHR

203 Robert Walker, 'The English Law of Privacy–An Evolving Human Right' < https://www.supremecourt.uk/docs/speech_100825.pdf> accessed 14 March 2021.
204 See Walter F. Pratt, *Privacy in Britain* (Associated University Press, Delaware, 1979) 38–59: Raymond Wacks, *Personal Information: Privacy and the Laws* (Claredon Press, Oxford, 1993).
205 Laura Lee Mall, 'The Right to Privacy in Great Britain: Will Renewed Anti–Media Sentiment Compel Britain to Create a Right to Be Let Alone' (1998) 4 (2) ILA Journal of International Comparative Law, 35.
206 Article 8 of the Convention provides that, everyone shall have the right to respect for his private and family life, his home and his correspondences.
207 Article 12 provides that, 'No one shall be subjected to arbitrary interference with his privacy, 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.'
208 Oliver Diggelman and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 Human Rights Law Review, 441–458.
209 Diggelman and Cleis (n 212) 441.
210 Gordon Brown, *The Universal Declaration of Human Rights in the 21st Century: A Living Document in a Changing World* (Open Book Publishers, Cambridge, 2016) 2.
211 Mary Ann Glendeon, The Rule of Law in the Universal Declaration of Human Rights' (2004) 2(1) North Western Journal of International Human Rights, 4.

provides that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[212]

In almost identical terms, article 17(1) of the International Covenant on Civil and Political Rights (ICCPR) which Nigeria ratified in 1993 guarantees the right to privacy thus: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondences or unlawful attacks on his honour and reputation.' The distinguishing factor between both conventions being that, while the UDHR is not legally binding,[213] the provisions of ICCPR have binding effect that guarantees protection from indiscriminate intrusion into private spaces.[214]

In Nigeria, chapter 4 of the extant 1999 Constitution houses fundamental rights[215] which have been defined by the Supreme Court as 'rights which stand above the ordinary laws of the land and which are in fact antecedent to the political society itself and it is a primary condition to civilized existence.'[216] As part of the fundamental rights enjoyable by citizens, the extant 1999 Constitution guarantees right to privacy as: 'privacy of citizens, their homes, correspondences, telephone conversations and telegraph communications, is hereby guaranteed and protected.'[217]

212 The provision guarantees right to privacy on one hand and right to private and family life on the other. See Antoon De Baets, 'The Impact of the Universal Declaration of Human Rights on the Study of History' (2004) 48(1) History and Theory, 20–43.
213 Syed Hassan, The 'Declaration' in UDHR' (2020) < https://www.researchgate.net/publication/340236754_THE_'DECLARATION'_IN_UDHR> accessed 3 April 2021.
214 Oliver Diggelman and Maria Nicole Cleis 'How the Right to Privacy Became a Human Right' (2014) 14 Human Rights Law Review, 449.
215 Constitution of the Federal Republic of Nigeria, 1999 (As Amended) C.23 Laws of the Federation 2004 (1999 Constitution)
216 Olumide Babalola, Babalola's Law Dictionary of Judiciary Defined Words and Phrases (2nd edn Noetico Repertum, Lagos, 2019) 117: Ransome–Kuti v Attorney General of the Federation (1985) 2 NWLR (Pt.6) 211 Badejo v Minister of Education (1996) 9–10 SCNJ 51.
217 Section 37, Constitution of the Federal Republic of Nigeria, 1999 (as amended).

For a clearer understanding and appreciation of the dynamics of right to privacy under the section 37 of the 1999 Constitution, it can be broken down into the following components: (a) privacy of citizens; (b) privacy of homes; (c) privacy of correspondences; (d) privacy of telephone conversations: (e) privacy of telegraph communication; and (f) privacy of family life.

Privacy of citizens. The Nigerian Court of Appeal admitted in *Nwali v EBSIEC* that the Constitution provides no definition or interpretation for the phrase "privacy of citizens' but it must not be given a restrictive or narrow meaning[218]and in addition, the Constitution does not define the word 'citizen' but provides some clarity on how citizenship can be acquired thereby perhaps eliminating any lingering doubts on the concept under the Nigerian law.[219]

The Supreme Court has however defined privacy to mean a right to protect one's thought, consciences or religious belief and practice from coercive and unjustified intrusion and one's body from unauthorized invasion.[220]

This right has been described as 'the most comprehensive of right and the most valued by civilized men' and broad enough to accommodate as many private concerns of individuals as possible.[221]It is the right of citizens to set boundaries on what extent of their opinions, feelings, beliefs, thoughts they voluntarily desire to share or expose to others and it also implies a citizen's choice to share or withhold intimate information from others.[222]

218 (2014) LPELR–23682(CA), per Agim, JCA, pp. 35.
219 Emmanuel Kelechi Iwuugwu, 'The Concept of Citizenship; Its Application and Dental in the Contemporary Nigerian Society' (2015) 8(1) International Journal of Research in Arts and Social Sciences, 165.)
220 Medical and Dental Disciplinary Tribunal v Okonkwo (2001) LPELR–1856(SC), see also the Court of Appeal decision in Enyinnaya v State (2014) LPELR 22924 (CA) where privacy was defined as 'right to be left alone.'
221 Sabah Al–Fedaghi, 'The Right to be let Alone' and Private Information' in Chin–Sheng Chen, Joaquim Filipe, Isabel Seruca and José Cordeiro, (eds) *Enterprise Information Systems VII* (Springer International Publishing, 2007).
222 Dorothy J. Glancy, 'The Invention on Right to Privacy' (1979) 21(1) Arizona Law Review, 2.

Ultimately the conception of this privacy is traceable to the 1890 article of Warren and Brandeis wherein, they argued that, unjustifiable intrusion and interference with private information, emotional life, thought and emotions deserved legal protection under what they termed 'right to be let alone' which metamorphosed into modern day right to privacy.[223] Hence, from an aggregation of judicial interventions, privacy of citizen is the right of citizens to be left alone and protection of their private affairs (ie thought, conscience religion, beliefs and bodies) from unjustifiable interference, intrusion or invasion.

Privacy of homes. This principle is built around Sir Edward Cokes' (castle doctrine) ruling in Semanyne's case that:

> *"The house of everyone to him is his castle and fortress, as well as for his defense against injury and violence as for his repose and although the life of a man is a thing precious and favoured in law so that, although a man kills another in his defense or kills one per infortunium (by misfortune) without any intent, yet it is felony and in such case, he shall forfeit his goods and chattels for the great regard which the law has to a man's life but if thieves come to a man's house to rob him or murder and the owner or his servants kill any of the thieves in defense of himself and his house, it is not a felony, and he shall lose nothing…"*[224]

The ruling above shows the high premium placed on privacy and defense of home by law to protect citizens' home from all forms of unjustifiable intrusion and invasion as far back as the sixteenth

223 Ben Bratman, 'Brandeis and Warren' The Right to Privacy and Birth of the Right to Privacy (2002) 69 Tenn. Law Review 623.
224 (1604) All ER Rep 62, (1604) 77 ER 194.

century when the Seymane's case was decided.[225]

The doctrine took off as homeowners right to protect their properties from invasion but gradually metamorphosed into what Al–Fedaghi[226] describes as active privacy right which sparked political debates on whether citizens could use reasonable force to ward off home privacy invasion in the US.[227] This principle insulates citizens from indiscriminate and unlawful searches of homes and seizure of properties, eavesdropping, surveillance or monitoring of conversations in private spaces.[228] In 2001, the US Supreme Court affirmed that, an individual has a reasonable expectation of privacy in his/her home which prohibits the government from embarking on unjustifiable searches even with the use of new technology that did not physically enter the home.[229] Article 8 of the European Convention on Human Rights makes similar to the provision of section 37 of the Nigerian Constitution in relation to privacy of home. This constitutional protection afforded sanctity of homes was engendered by judicial hesitation to interfere in domestic affairs.[230] The European Court of Human Rights (ECtHR) has defined 'home' to include business premises and in a wider sense as a 'domicile' and the search of business premises interfered with respect for home.[231] The court also observed that the searches of press premises of journalists for the purpose of obtaining information interfered with privacy

225 Justice Thomas M. Cooley, *A Treatise of the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union* (4th edn, Brown & Co., Boston, 1871).
226 Al–Fedaghi (n 221).
227 Tyler Anderson, 'Balancing the Scales: Re–Instating Home Privacy Without Violence in Indiana' (2013) 88(1) Indiana Law Journal 391. See also American decisions in Barnes v State 946 N.E 572 (Ind. 2011), People v Tomlins 107 N.E. 496 (N.Y. 1914), Beard v United States 158. U.S 550 (1895).
228 Daniel B. Yeager, 'Search, Seizure and Positive Law: Expectations of Privacy Outside the Fourth Amendment' (1993) 84(2) Journal of Criminal Law and Criminology, 249.
229 Kyllos v United States 533 U.S. 27. (2001).
230 See Jonathan L. Hafetz, 'A Man's Home is His Castle? Reflections on the Home, the Family and Privacy During the Late Nineteenth and Early Twenties Centuries' (2001–2002) 8(2) William & Mary Journal of Women and the Law, 175.
231 See Niemetz v Germany, 16 December 1992, 29–33, series A no. 251 251 B, Tamosius v United Kingdom, no. 62002100 ECHR 2002, Sallinen and Others v Finland no.50882199, 71, 27 September 2005 and Case of Wiesner and Bicos Beteileigungen GmbH v Austria no. 74336101, 16 January 2008.

of home.[232]

The word 'home' has been given various meanings; it has been viewed as a psychological concept which gives a sense of belonging to a person. A physical space that influences the mental and physical needs of an individual.[233] Fox in her comprehensive article on the conceptual attempts at defining or describing the term noted that, 'home' can be viewed as 'a physical structure which offers material shelter; 'a territory which provides security and control, locus in space, permanence, continuity and privacy'; 'a centre for self–identity which offers reflection on one's idea and values and acts as indicator of personal status'; 'a social and cultured unit that acts as the locus for relations hope and family and friends.'[234] The home is a centre of emotional significance of familiarity and belonging[235] but whereas physical structure is not a necessary feature, it could find expression in any 'existential space' such as neighbourhood, village, city, town, state or country.[236] Home has also been described as a crucial site of cultural activity and cultural expression,[237] hence, builders and other professionals have the propensity of addressing 'house' as 'home' but in the context of privacy claims, it may be jurisprudentially costly to conflate both concepts,[238] nevertheless, it is however conceded that, in certain circumstances, a house may serve both purposes.[239]

The Nigerian courts have had cause to enforce privacy of home in a

232 Roemen and Schmit v Luxembourg (application no. 51772/99) 25 February 2002.
233 Masran Saruwono, 'Shouting in Silence: Expression of Self in Private Homes' (2021) 42 Procedia Social and Behavioural Sciences, 1.
234 Lorna Fox 'The Meaning of a Home: A Chimerical Concept or Legal Challenge' (2002) 29(4) Journal of Law and Society, 580–610.
235 Yi–Fu Tuan, 'Place. An Existential Perspective (1975) LXV The Geographical Review, 151–165.
236 Christian Norberg–Schulz, *Genius Loci: Towards a Phenomenology of* Architecture (Rizzoli, New York,1980).
237 Judith Sixsmith, 'The Meaning of Home: An Explanatory Study of Environmental Experience' (1986) 6 Journal of Environmental Experience 281–298.
238 R.D. Cramer, 'Images of Home' (1960) XLVI Journal of the American Institute of Architects, 40–49.
239 Judith Sixsmith, 'House and Home in Old Age' (1985) Paper Presented at British Society of Gerontology Conference, Keele University.

number of cases where the invasion mostly concerned invasion of physical structures. For example, in *Ojoma v State*, [240] the invasion of a native doctor's house was deprecated being a violation of his privacy of home and in *Ibrahim v Nigerian Army*[241] where a senior army officer entered his junior's home and cohabited with his wife, the Court of Appeal ruled same as a violation of the junior's privacy of home.[242]

With the advancement in technology permeating most human endeavours, privacy of homes now extends to smart homes.[243] Technology now enables invasion of privacy without physical intrusion or invasion of such homes and the increasing dependence of homes on internet–enabled devices is directly proportional to the growing rate of privacy and security risks that the residents of such homes are exposed to.[244] Smart homes stand the risk of remote attack by a cyber–attacker who can hack the networks and access private information like bathing, sleeping or sexual activities.[245] Intrusion of privacy of smart homes could also take the form of control–hijack where a scrupulous attacker remotely wrestles control of the smart home devices for untoward use.[246]

Ultimately privacy of home under section 37 of the Nigerian

240 (2014) LPELR–22942 (CA).
241 (2015) LPELR–24596 (CA).
242 It is worthy of note that section 45 of the Constitution provides for derogation of privacy in certain circumstances. For instance, the Court of Appeal noted in Enyinnaya v State (2014) LPELR 22924 (CA) that privacy, can be derogated by a law enacted in the interest of defence, public safety, public safety, public order, public morality, public health or in protecting others fundamental rights.
243 These are residences equipped with computing and information technology which anticipate and respond to the needs of the occupant(s). These modern homes are built with technology–driven functionalities that ease in–house seamless control of gadgets and appliances, communications, home care, catering and entertainment, security and energy needs etc. See Frances Aldrich, 'Smart Homes' Past, Present and Future' in Richard Harper (ed) *Inside Smart Homes* (Springer International Publishing, New York, 2008); Andreas Jacobson, Martin Boldt and Bengt Carlsson, 'A Risk Analysis of a Smart Home Automation System (2016) Future Generation Computer Systems, 719–733.
244 J. Sturgess, J.R.C. Nurse and J. Zhao, 'A Capability Oriented Approach to Assessing Privacy Risk in Smart Home Ecosystems' (2018) Conference paper at Living in the Internet of Things, Cybersecurity of IOT.
245 Bako Ali and Ali Ismail Awad, 'Cyber and Homes (2018) 18(3) Sensors, 817.
246 Joseph Bugeja, Andreas Jacobsson and Paul Davidsson, 'On Privacy and Security Challenges in Smart Connected Homes (2016) European Intelligence Security Informatics Conference.

Constitution implies sanctity of home and its protection from unauthorized intrusive activities like unlawful searches and seizures, eavesdropping, surveillance, monitoring etc.

Privacy of correspondence: (secrecy of correspondence).

Correspondence is defined as 'letters, especially official or business letters' and 'the action of writing, receiving, and reading letters, especially between two people.'[247] The foundation of this specie of privacy is closely–linked to the American pre–independence postal system institutionalized in response to British monopoly, monitoring and surveillance activities as well as censorship.[248] Secrecy (privacy) of correspondence had been given paramount consideration in the comity of nations since the eighteen century when twenty (mostly) European countries under the leadership of France, participated in the 1865 International Telegraphic Conference to discuss and regulate the handling of international telegraphic traffic with the main objective of promoting privacy of correspondence by guaranteeing secrecy of telegraphic dispatches.[249] On the importance of this on the development of privacy of correspondence, Powers notes that, 'the historic role of secrecy in international relation has clear and direct application to contemporary debates about privacy and surveillance.'[250]

In a number of decisions, the ECtHR has repeatedly considered privacy of correspondence thereby giving the concept an interesting measure of clarity in the process. In *Barbulescu v Romania*, the court found that telephone calls are within the meaning of

247 Cambridge Advance Learner's Dictionary (3rd edn, Cambridge University Press, Cambridge, 1995).
248 Robert G. Natelson, 'Founding–Era Socialism; The Original Meaning of the Constitution Postal Clause' (2018) 7(1) British Journal of American Legal Studies, 15.
249 International Telecommunications Union, 'Paris, 1865: The Birth of the Union' < http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/12.36.72.en.100.pdf> accessed 4 April 2021.
250 Shan Powers, 'Where did the Principle of Secrecy in Correspondence Go?' (2015) The Guardian < https://www.theguardian.com/technology/2015/aug/12/where–did–the–principle–of–secrecy–in–correspondence–go> accessed 10 April 2021.

correspondence and the notion also covers correspondence of a professional nature[251] or within a business environment.[252]

The right guarantees confidentiality and sanctity of information exchange involving citizens on whatever form or mode irrespective of circumstances of such communications. For instance, the ECtHR ruled in the case of *Silver and Others v United Kingdom*[253] that the right enures to the protection of a prisoner. In that case, seven prisoners sued the UK government alleging that the control of their mails by the prison authorities interfered with their privacy of correspondence and court agreed that the stoppage or delay of their letters violated their rights to privacy of correspondence. Also, in *Mehmet Nuri Ozen v Turkey,*[254] where prison authorities refused to dispatch letters written by prisoners in languages other than Turkish, the ECtHR ruled that the refusal interfered with the prisoners' right to privacy of correspondence guaranteed by article 8 of the European Convention on Human Rights.

Under European human rights law, the term 'correspondence' includes parcels confiscated by border control agencies or customs,[255] telephone conversation between family members or others, [256] telephone conversations from business premises.[257] With the advancement in technology, electronic and digital exchange of information are also covered by the notion of correspondence

251 Niemietz v Germany, 16 December 1992, 29, series no 251.
252 Liberty v. France (no 588/13) February 2018.
253 No. 5947172) 25 March 1983.
254 (No. 15672108) 11 January 2011.
255 X v United Kingdom (no. 7215/75) 12 December 1978.
256 Margareta and Roger Anderson v Sweden (No. 61/1990/253/323) 20 January 1992.
257 Amann v Switzerland (no. 27798/59) 11 February 2000; Halford v United Kingdom (no. 20605/92) 25 June 1997); Copland v United Kingdom (no. 62117/00) 3 April 2007 and Kopp v Switzerland (no. 13/1997/797/1000) 25 March 1998.

which has been extended to include cloud computing.[258] It has been observed that 'resource monitoring' in cloud computing raises issues of privacy of correspondence, hence the non–physical nature of correspondences in cloud computing does not preclude it from the ambit of secrecy of correspondence.[259]

In *Copland v United Kingdom*, an employee's e–mails and internet usage were monitored to elicit certain personal information, the ECtHR agreed that there had been a violation of her privacy of correspondence[260] and in *Wieser's case*, a search of computer servers and storage systems where a lawyer's correspondence were retrieved was held to have violated his privacy of correspondence.[261]

In the same manner, this principle was applied to searches and retrieval of correspondences from hard drives, floppy disks,[262] telex, pager messages[263] but it should be noted that, since the meaning of correspondence limits its scope to an exchange of information between a certain number of identifiable people (the maker and the recipients), broadcasts of any kind to the public at large would not constitute correspondence within the context of privacy of correspondence.[264] Privacy correspondence could be violated in many ways: opening and reading a folded

258 Cloud computing is a term for modern technology that provides on–demand and seemless 'network to access to shared pool of configurable computing resources.' See Yunchun Sun, Junsheng Zhu, Yongpin Xiong and Guangyu Zhu 'Data Security and Privacy in Cloud Computing' (2014) International Journal of Distributed Sensor Networks 9. It has been described as simultaneous or ubiquitous data centres available to many consumers on the Internet. See Piter Mell and Tim Grance 'The NIST Definition of Cloud Computing' (2009) 53(6) National Institute of Standards and Technology, 2. In cloud computing, users are able to remotely access and utilize a network of servers hosted on the internet for processing (alternating, transmission, management, creation, storage etc. of data as opposed to the performance of those activities locally or on personal devices. See Ishrat Ahmad, 'Cloud Computing–A Comprehensive Definition' (2017) < https://www.researchgate.net/publication/314072571_Cloud_Computing_–_A_Comprehensive_Definiton> accessed 12 April 2021.

259 Yunchun Sun, Junsheng Zhu, Yongpin Xiong and Guangyu Zhu 'Data Security and Privacy in Cloud Computing' (2014) International Journal of Distributed Sensor Networks, 9.

260 No. 62117/00, 3 April 2007.

261 Wieser and Bicos Beteiligungen GmbH v. Austria (no. 74336/01) 16 October 2007.

262 See Petri Sallinen and Others v Finland (50882/99) 27 September 2005. 27 September 2005,

263 Christie v United Kingdom (21482/93 27 June 1994); X and Y v Belgium (no. 8962/80 13 May 1982 and Taylor–Sabori v United Kingdom (no.47114/99) 22 October 2002.

264 B.C. v Switzerland (no. 21353/93) 27 February 1995.

piece of writing (letter),[265] preventing a citizen from initiating correspondence,[266] screening correspondence,[267] duplicating correspondence,[268] detection of a portion of correspondence,[269] and forwarding mail to a third party.[270]

I am not aware of any Nigerian court decision that specifically ruled on issue of privacy of correspondence however a decision that comes close is found in the decision in *Registered Trustees of Nigerian Bar Association (NBA) v Attorney General of the Federation and Anor*.[271] where the plaintiff successfully challenged the requirement for Nigerian lawyers to report their transactions with clients up to a certain threshold to an anti–corruption office on the ground that such reports would interfere with privacy of correspondences under section 37 of the Constitution, among other grounds. The court however decided the case in favour of the NBA on other grounds apart from privacy.

Privacy of telephone conversations. This is similar to privacy of correspondence but for the specificity of telephone communications. The Nigerian Constitution guarantees freedom to have telephone conversations without interference from any quarters and the provision protects all manner of telephone conversations irrespective of its contents except derogated by law.

The ECtHR has ruled on activities that constitute interference with privacy of telephone conversations to wit: interception of

265 A. v France (no. 14838/89 23) November 1993; Frerot v France (no. 70204/01) 12 June 2007; Laurent v France (no. 28798/13) 24 May 2018; Narinen v Finland (no. 5027/98) 1 June 2004; Idalov v Russia (No. 5826/03) 22 May 2012.
266 Golder v United Kingdom (no.4451/70) 21 February 1975.
267 Campbell v United Kingdom (no. 13590/88) 25 March 1992.
268 Foxley v United Kingdom (no. 33274/96) 20 June 2000.
269 Pfeifer and Plank v Austria (no. 10802/84) 25 February 1992.
270 Luordo v Italy (2003) ECHR 372. See generally Council of Europe' 2018 Guide on Article 8 of the European Convention of Human Rights.
271 FHC/ABJ/CS/173/2013. The Defendants appealed to the Court of Appeal and their appeal No. CA/A/202/2015 was dismissed on 14th day of June 2017.

telephone calls,[272] telephone tapping or wiretapping,[273] metering of telephone lines,[274] and storage of interrupted telephone data etc.[275]

In *Emerging Markets Telecommunication Services v Eneye*[276] unsolicited text messages sent to a subscriber's telephone line were adjudged an interference with his privacy of telephone line. The court found that the telecommunication company shared the subscriber's personal telephone number with third parties without his consent and that, the spam messages received from such entities constituted an infringement. [277] Thus, it would be seen from the decision that, the telecommunication company was not held liable for sending the messages but for sharing the subscriber's telephone line with unknown interferring entities who sent the spam text messages and thereby interferring with privacy guaranteed under section 37 of the Constitution.[278]

Privacy of telegraphic communications. The public telegraph became a prominent means of telecommunication in the eighteenth century when it was introduced into Nigeria by the colonial administration.[279] The telegraph was used to transmit information 'coded signals' and it was the major means of communicated information by wire or radio wave in the 18th century upwards. Telegraph was used as a means of correspondence, hence the principles and decisions applicable

272 Amann v Switzerland (no. 27798/95) 16 February 2000.
273 Malone v United Kingdom (no. 8691/79) 2 August 1984.
274 P.G and J.H v United Kingdom (no. 44787/98) 25 September 2001; Lambert v France (no. 88/1997/872/1084
275 Copland v United Kingdom (no. 62617/00) 3 April 2007; See Tudurachi Elena 'Wiretaps Interference of Public Authorities in the Right to Privacy' (2014) Procedia–Social and Behavioural Science, 4591–4595.
276 (2018) LPELR–46193(CA).
277 See Oluwaseun J. Akanji and Bamidele S. Adeleke, 'Subscribers Attitude Towards Unsolicited Text Messages (UTM) Among Nigerian Telecommunication Firms' (2018) 3(3) European Journal of Management and Marketing Studies, 33; Basheer A.M. Al–lak. And Ibrahim A.M. Alnawasi, 'Mobile Marketing: Examining the Impact of Trust, Privacy Concern and Consumer's Attitude on Intention to Purchase' (2010) 5(3) International Journal of Business and Management, 29.
278 See also similar decisions on unsolicited telephone calls in Godfrey Eneye v MTN Nigeria (unreported) (CA/L/136/2009); Anene v Airtel Nigeria (Unreported) FCT/HC/CV/545/2015 and Joshua Agbi v MTN Nigeria (unreported) Suit No. FHC/L/CS/456/2018.
279 Anthony A. Ijewere and E.C. Gbandi, 'Telecommunications Reform in Nigeria. The Marketing Challenges (2012) 10(2) JORIND 194.

to 'privacy of correspondence' apply mutatis mutadis. McMullan notes that, with the invention of electronic telegraphy came the risk of privacy violations thus:

"For the vast majority of human civilisation, the scope of day–to–day conversational privacy had pretty much been whatever was beyond earshot. But the rise of the telegraph meant that the possibilities of communication exploded; by the mid–19th century you could go to a telegraph station and have a message sent further and faster than had ever been possible. The whole idea of what was "beyond earshot" changed inexorably. Along with that expanded space of communication came a newfound vulnerability. Words could be snatched from you long after they'd left your vicinity. Electrical telegraph lines could be tapped, signals intercepted. Cable workers were required to sign confidentiality agreements, but even they could be bribed to divulge messages."[280]

Private and Family Life.

The phrase 'private and family life' has two broad limbs with wider coverage than right to privacy.[281]In the English case of *Costello–Roberts v United Kingdom,* [282] it was observed that the phrase is incapable of exhaustive definition rather, the court held that it would be too restrictive to limit the notion of private life to 'inner circles' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside would not encompass within that circle. Private and family life is broader and more comprehensive than right to privacy as the former includes the right to establish and develop relationships

280 Thomas McMullan, 'The World's First Hack: The Telegraph and the Invention of Privacy' (2015) < https://www.theguardian.com/technology/2015/jul/15/first–hack–telegraph–invention–privacy–gchq–nsa> accessed 1 July 2021.
281 Alan Desmond, 'The Private Life of Family Matters: Curtailing Human Rights Protection for Migrants under Article 8 of the ECHR?' (2018) 29(1) European Journal of International Law, 261–279.
282 No. 1313/87. 25 March 1993.

with other persons and the outside world.[283]

Unlike article 8 of the European Convention on Human Right which expressly provides for the rights to respect for private and family life in the text of the body of the treaty, the provision of section 37 of the Nigerian Constitution 1999 does not guarantee right to private and family life, it merely confines the phrase to the table of contents and marginal note.[284] In *Uwaifo v Attorney General of Bendel State*[285], the Supreme Court observed that, marginal notes or explanatory notes ought to be ignored as they only offer explanation to statues and nothing more. The grave implication of omission of the phrase 'private and family' life is that the extant constitution does not guarantee a 'right to private and family life' since no such provision exists in the body of the Constitution, especially since marginal notes are meant to be ignored in the interpretation of statutes.[286]

It is conceded that Nigerian courts have repeatedly quoted the phrase 'private and family life' but such reference has been, with respect, without constitutional basis since the marginal notes do not from part of the Constitution as reiterated by the Supreme Court in *Akintokun v LDPC.*[287]

283 Ursula Kilkelly 'The Right to Respect for Private and Family Life' Human Rights Handbook No. 1' (2001) Council of Europe, 2001.
284 See Olumide Babalola 'Does the Nigerian Constitution expressly provide for a 'right to private and family life'?: Re–interrogating the effect of the marginal note in section 37 of the Constitution of the Federal Republic of Nigeria 1999' https://esq–law.com/does–the–nigerian–constitution–expressly–provide–for–a–right–to–private–and–family–life.html accessed 13 April 2021.
285 (1987) 7 SC 124.
286 (The Supreme Court expressly held that marginal notes do not form part of enactment, see Yabugbe v C.O.P (1992) LPELR–3505 (SC).
287 (2014) LPECR–22941(SC).

CHAPTER SIX

Evolution of data protection in Nigeria

In this book, the term 'data protection' is distinguishable from privacy and they are not used interchangeably because the unidentical twin concepts are similar but also different in many respects.[288] However, the term 'data protection' is used interchangeably with 'data privacy' in this book even though while no international instrument has adopted the term 'data privacy,' notable scholars have adopted the term in their respective academic interventions.[289] In spite of its international legislative 'snub' an Asian country has enacted her data protection legislation with such nomenclature thereby giving the term some legislative validation.[290] Ultimately, the adoption of 'data privacy' or 'data protection' appears a matter of semantics rather than substance or form.

Bygrave defines data protection law as rules that 'specifically

288 Paul de Hert and Eric Schreuders,'The Relevance of Convention 108' 33,42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw 19–20 November 2001. The relationship and interplay of both concept is discussed in a later chapter.

289 See Christopher Kunar, Transborder Data Flows and Data Privacy (Oxford Scholarship Online, 2003); Lee A. Bygrave, Data Protection Law: An International Perspective (Oxford University Press, 2014); Alex B. Makulilo, African Data Privacy Laws (Springer International Publishing, New York, 2016); Gregor Dorfleitner and Lars Hornuf, Fintech and Data Privacy in Germany (Springer International Publishing, New York, 2020); Theo Lynn, John G. Mooney, Lisa van der Werff and Grace Fox, Data Privacy and Trust in Cloud Computing (Palgrave McMillan, London, 2020). In some jurisdictions (the US, for example), the term data privacy is preferred because data protection laws do not aim to protect data rather the interest of data subjects concerned. See Paul Schwartz 'Data Processing and Government Administration: The Failure of American Legal Response to Computer' (1992) Hastings Law Journal, 1321.

290 See the Philippines Data Privacy Act No. 10173 of 2012.

regulate all or more stages in the processing of personal information,'[291] while De Hert and Gutwirth argue that they represent 'a catch–all term for a series of ideas with regard to the processing of personal data.'[292] Tzanou says the data protection refers to 'a set of legal rules that aim to protect the rights freedom and interests of individual whose personal data are collected, stored processed, disseminated, destroyed etc,'[293] and then Blume defines the concept as the 'legal rules that regulate to which extent and under which conditions information related to individual physical persons may be used.'[294] Roos notes that data protection is 'the legal protection of a person (called the data subject) with regard for processing of data concerning him or herself by another person or institution (called the data–controller).[295] The description or definition of data protection is however often coloured from many perspectives of the proponents and it may be seen from diverse points of view to wit: as a tool of informational control and privacy,[296] regulation of risks of technological incursion in businesses and other human interactions etc.[297]

The term, 'data protection' was historically curled from the title of the first modern data protection law–'Datenschutzgesetz' enacted on the 13th day of October 1970 by the German State of Hessen as drafted by Prof. Spiros Simitis–regarded as one of the pioneers of

291 Lee A. Bygrave Data Protection Law: Approaching its Rationale, Logic and Limits (Kluwer Law International, Holland, 2002) 2.
292 Paul de Hert and Serge Gutwirth, Data Protection in the Case Law of Strasbourg and Luxembourg: Constitution in Action in Reinventing Data Protection? (Springer International Publishing, New York, 2009) 3.
293 Maria Tzanou, 'Data Protection as a Fundamental Right, Next to Privacy? 'Reconstructing a Not so New Right' (2013) 3(2) International Data Privacy Law, 88–89.
294 Peter Blume 'Data Protection and Privacy–Basic Concepts in a Changing World' (2010) Scandinavian Studies in Law, 151.
295 Anneliese Roos, 'Core Principle of Data Protection Law' (2006) 39(1) Computer and International Law Journal of Southern Africa 102–130.
296 Viktor Mayer–Schönberger, 'Generational Development of Data Protection in Europe,' in P. E. Agre & M. Rotenberg (eds) in *Technology and Privacy: The New Landscape* (MIT Press, London 1998) 219–241.
297 Raphael Gellert, 'Understanding Data Protection as a Risk Regulation' (2015) 18(11) Journal of Internet Law, 3–16.

data protection.[298] The term 'data protection' has however been widely criticized as being a misnomer since the law protects the rights of data subjects rather than their data itself, hence, some stakeholders preferred the term 'privacy protection law' but this semantic preference was not without its own set of criticisms.[299]

Early conversations around data protection are also traceable to a foremost case in 1983, wherein the German Constitutional Court in its landmark decision (the census case) annulled the population Census Act and upheld an individual's right to 'informational self–determination' which empowers such individual to control the transmission or otherwise use of his personal data.[300] On the events that led to the enactment of the world's first modern data protection legislation,[301] Simitis accounted that:

> *"Databanks, like the collection initiated by the Government of the German Federal State of Hesse in the middle of the 1960s, embodied the hopes evoked by "cybernetic machines." The data collections were to allow efficient long–term policies, such as in finance and social security, and also to secure better medical help, especially in emergencies. But while the databanks were at first generally accepted, doubts gradually arose, beginning in 1968, with regard to the processing of personal data. The involvement of nearly all*

298 See Christoph Klug. 'Spiros Simitis, Bundesdatenschutzgesetz,' (2012) 2(2) International Data Privacy Law, 113; Douwe Korff and Marie Georges, 'The Origins and Meaning of Data Protection' (2020) <https://ssrn.com/abstract=3518386> accessed 7 April 2021. Prof. Simitis became the world's first Data protection Commissioner in 1970 when he, alongside others, pioneered the first modern data protection law in the German state of Hessen. See Colin J. Bennet, The Privacy Advocates: Resisting the Spread of Surveillance (Massachusetts Institute of Technology, 2008) 76.

299 Eleni Kosta, *Consent in European Data Protection Law*, (Martinus Nijhoff Publishers, Leiden, 2013) 46.

300 Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self–Determination' (2009) 25(1) Computer Law & Security Report, 84–88.

301 The Hessen Data Protection Act was followed by the Swedish Data Protection Act in 1973. See Tore Dalenius, 'Data Protection Legislation in Sweden: A Statistician's Perspective' (1979) 142(3) Journal of the Royal Statistical Society, 285–298.

> *Hesse citizens, the storage of especially sensitive data, as those concerning health or income, and the databank's capacity to exploit information for different purposes triggered demands that the Government investigate the risks of a permanent surveillance of citizens. Consequently, on October 10, 1970, the Hessian Parliament adopted the world's first Data Protection Act after a short but intensive debate."*[302]

It must be however noted that while the Hessen Act was the first modern data protection law, the Swedish Data Act enacted in 1973 was the world's first national data protection law.[303]

In Nigeria's case, data protection does not have a colourful trajectory as far as the development of the concept is concerned. In 2007, the Nigerian government set up the current national statistics system pursuant to the Statistics Act[304] to increase public awareness on data usage, and processing activities etc.[305] The increased utility of technology in the country also saw the rise in processing activities necessitating direct legal protection and like all other countries, Nigerians became increasingly reliant on technology for every facet of their lives, hence the need to proactively address privacy and data protection issues since technology was daily used to facilitate exchange of personal data for business and all other purposes.

While the right to privacy has been recognised as one of the indispensable fundamental rights from time immemorial, data

302 Spiros Simitis, 'Privacy–An Endless Debate?' (2010) 98(6) California Law Review, 1989, 1995.
303 Soren Oman, 'Implementing Data Protection in Law' (2004) 47 Scandinavian Studies in Law, 389–403.
304 No. 9 of 2007.
305 Olusanya Olubusoye, Grace Korter and Obafemi Keshinro 'Nigerian Statistical System; The Evolution, Progress and Challenges' (2015) < https://www.researchgate.net/publication/283715250_NIGERIAN_STATISTICAL_SYSTEM_THE_EVOLUTION_PROGRESS_AND_CHALLENGES >accessed 5 April 2021.

protection only became the world's major focus in the past decade or two, notwithstanding its discovery since the seventies.[306] The resultant effect of this is the enactment of legislation hinged on the data protection across various countries and this has obligated business to ensure due protection of customers' personal information from misappropriation or corruption, and by association, privacy protection of persons. The twin concept of data protection and privacy recalls two major schools of thought. The first of these has reasoned that data protection clings to privacy and should not be alienated from it but the reductionist school contends that data protection should be wholly detached from privacy.[307]

Nonetheless this area of philosophical disparity, it remains unlikely that the history of data protection can be unconnected to constitutional development in Nigeria and this may, unfortunately, persist until the Nigerian Supreme court determine the connection between privacy and data protection. Hence, this chapter concentrates on data protection with minimal reference to privacy even though most commentators on the issue agree that data protection originated from privacy.[308]

The concept of data protection in Nigeria is traceable to the country's wholesome embrace of technology for her business and private activities when her citizens' characteristic communal

306 Mercia Fynn, Data Protection and Privacy, (2021) Kisch <https://www.lexology.com/library/detail.aspx?g=ba02d5c9–943d–4073–aa34–8b8eadca9e3b&utm_source=lexology+daily+newsfeed&utm_medium=html+email++body++general+section&utm_campaign=lexology+subscriber+daily+feed&utm_content=lexology+daily+newsfeed+2021–04–23&utm_term=

307 Adekemi Omotubora & Subhajit Basu 'Next Generation Privacy' (2020) 29(2) Information & Communications Technology Law' 151–173.

308 See Lukman A. Abdulrauf and Charles M. Fombad, 'Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms' (2016) 38(2) Liverpool Law Review, Andrew U. Iwobi, 'Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime' (2016) 26(3) Transnational Law and Contemporary Problems 13, Yinka Olomojobi, 'Right to Privacy in Nigeria' (2017) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062603> accessed 17 March 2020, E.S. Nwauche 'The Right to Privacy in Nigeria' (2007) 1 CLAS Review of Nigerian Law and Practice, 66–90, Iheanyi Nwankwo, 'Nigeria's Data Privacy First Responders' (2018) < https://iheanyisam.wordpress.com/2018/04/04/nigerias–data–privacy–first–responders/> accessed 18 March 2021.

co–existence gradually caved–in to individualism[309] which precipitated the need for legal protection for private matters even though implied provisions on data protection had been included in successive constitutions in the mould of information privacy.

The evolution of data protection in Nigeria is however fraught with uncertainties pronounced by little or no documentation, failed legislative attempts, judicial indifference, and political mind games. Nevertheless, there is no doubt that, the rapid technological penetration brought data protection to the fore at the federal level. Unfortunately, the regulations and laws that followed were not of general application as many of them restricted the protection of data to specific sectors.

Some academics have postulated that the earliest legislative attempt at data protection regulation was the Computer Security and Critical Information Infrastructure Protection Bill 2005, but the main objectives of the abortive bill revealed it was substantially meant to criminalise 'illegal conducts against ICT systems' and cybercrime.[310] While a negligible clause masqueraded as a provision on consent and purpose limitation, the bill's ultimate aim was to prosecute offenders rather than provide remedies to victims of data breaches.[311] However, after its first unsuccessful legislative appearance at the national assembly in 2005[312], the bill resurfaced in 2011 but was withdrawn before completing its legislative cycle.[313]

309 Alex B. Makulilo, 'The Quest for Information Privacy in Africa' (2018) 8 Journal of Information Policy, 317.
310 Bernard O. Jemilohun and Timothy I. Akomolede, 'Regulations or Legislation for Data Protection in Nigeria? A Call for a Clear Legislative Framework' (2015) 3(4) Global Journal of Politics and Law Research, pp.1–16.
311 Ibrahim Yusuff, 'A Critical Review of the Computer Security and Critical Information Infrastructure Protection Bill 2005 as Nigerian Specific Cybercrime Legislation' (2015) < https://martinslibrary.blogspot.com/2015/03/a–critical–review–of–computer–security.html> accessed 9 March 2021.
312 See Uchenna Jerome Orji, *Cybersecurity Law and Regulation* (1st edn, Wolf Legal Publishers 2012) 508.
313 Uchenna Jerome Orji, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria' (2019) 24(1) Tilburg Law Review, 105–124.

The next verifiable legislative attempt can be traced to October 2008 when the Nigerian government, in conjunction with other African states, took tangible steps towards the eventual adoption of the Supplementary Act (A/SA.1/01/10) on personal data protection within ECOWAS at the 37th session of the authority of Heads of State and Government in Abuja on the 16th day of February 2010.[314] The Convention seeks to 'establish a legal framework of protection for privacy relating to collection, processing, transmission, storage and use of personal data… in Nigeria' and it ultimately led to proposed Data Protection Bill 2010 targeted at 'reducing' unauthorised processing and use of personal data and information without the prior consent of the data subjects.[315] The bill was hyped to be the first federal legislative proposal solely focused on data protection but unfortunately it was silenced after the first reading.[316]

However, another bill styled 'Data Protection Bill 2011' resurfaced a year later and was sponsored to the National Assembly, but the document regarded as poorly drafted and comparatively weak never got to the President for his assent.[317]

As part of the legislative trajectory of data protection in Nigeria, the Freedom of Information Act was passed in 2011 to make partial provision for protection of citizens' personal information from public disclosure without the consent of such citizen in certain circumstances[318] and in 2013, the National Information Technology Development Agency (NITDA) issued the 2013 draft

314 Abdullahi M. Abdulquadir, 'Regional Trade and the Challenges of Data Protection in West Africa' (2020) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770159> accessed 17 February 2021.
315 Abubakar S. Aliyu, 'The Nigerian Data Protection Bill: Appraisal, Issues and Challenges' (2016) 9(1) The Innovative Issues and Approaches in Social Sciences Journal, 48.
316 Iheanyi Samuel Nwankwo, 'The Status of Data Protection Reform in Nigeria' (2015) https://iheanyisam.wordpress.com/2015/02/25/the–status–of–data–protection–reform–in–nigeria/ accessed 16 March 2021.
317 Andrew U. Iwobi, 'Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime' (2016) 26(3) Transnational Law and Contemporary Problems, 13.
318 Section 14 of the Freedom of Information Act, 2011.

Guidelines on Data Protection but was never officially released.[319] Further efforts in form of the Data Protection Bill 2015 were made by the Federal House of Representatives, but it was either renamed or aborted at Senate and in 2016, the National Identity Management Commission (NIMC) proposed the Personal Information and Data Protection Bill with provisions bordering on the collection use and disclosure of personal information and sponsored same to the House of Representatives, but it did not pass legislative scrutiny.[320] In 2017, the then Speaker of House of Representatives sponsored another Data Protection bill which, just like its predecessors, never crossed the legislative hurdles. In that same year, some data protection clauses were inserted in the Credit Reporting Act which was also passed into law by the National Assembly in 2017 with one of its main objectives aimed at granting data subjects a measure of privacy, confidentiality, and protection of their credit information but like other statutes, it was specific in nature and only restricts itself to the protection of credit data and information.

Nonetheless, before the issuance of the NDPR in 2019, the Council of Europe hand–in–hand with the Federal Ministry of Justice and some other stakeholders, drafted the Data Protection Bill 2018 and it was finally ready to be passed into law in 2019. However, assent was withheld by the President and that singular act reverted the country to square one in her quest to enact a principal law on data protection.[321] In 2020, the Federal Government of Nigeria through NIMC and NITDA invited the general public to make comments on a proposed draft Data Protection Bill 2020 but

319 Uche Val Obi, 'An Extensive Article on Data Privacy and Data Protection Law in Nigeria' (2020)https://eurocloud.org/news/article/an–extensive–article–on–data–privacy–and–data–protection–law–in–nigeria/ accessed 1 February 2021.
320 National Identity Management Commission, "Request For Comments and Observations on Draft Data Protection and Privacy Bill, 2018 and Invitation To 1–Day Validation Workshop' https://nimc.gov.ng/docs/draft_dataProtection_%20privacyBill.pdf accessed 21 April 2021.
321 Ife Ogunfuwa, 'Experts Call on Buhari to Assent Data Protection Bill' (2020) < https://punchng.com/experts–call–on–buhari–to–assent–data–protection–bill/> accessed 1 March 2021.

after the validation workshop was held in September of that year, nothing was heard about the bill before this book went to the press.

The preceding chronicle shows the many failed attempts by the Nigerian State to enact a principal data protection legislation before the makeshift[322] issuance of the Nigeria Data Protection Regulation (NDPR) in 2019. Notwithstanding its pitfalls, the NDPR is the most comparatively comprehensive piece of (subsidiary) legislation on data protection in Nigeria as of August 2021.

322 The World Bank refers to the regulation as a 'stopgap.' See World Bank, 'Nigeria Digital Economy Diagnostic Report' <http://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria–Digital–Economy–Diagnostic–Report.pdf> accessed 17 May 2021.

CHAPTER SEVEN

Sources of data protection law in Nigeria

NIGERIA'S RELATIONSHIP WITH Britain explicably influenced the nature and sources of the former's laws and practices[323] which derived from the doctrines of common law and equity. However, the major source of data protection in Nigeria is traceable to her Constitution(s),[324] other enactments by the legislature and international treaties and regulations.[325] In this chapter, the sources of Nigerian data protection law will be discussed under the following sub–headings:

- International instruments
- General legislation (substantive and subsidiary), and
- Sector–specific legislation.

i. International instruments

Data protection is a global concern regulated by a number of international treaties[326] but while there is no all–encompassing international treaty that universally regulates data protection, some international instruments influence privacy laws globally

323 Charles Nwalimu, *Nigerian Legal System* (Vol 1. Peter Lang Publishing, New York, 2007) 5; A.E.W. Park, *The Sources of Nigerian Law* (Sweet and Maxwell, London, 1963) 1.

324 Starting from the Nigeria (Constitution) Order 1954 (Lyttleton Constitution) which guaranteed right to privacy in its sixth schedule among other fundamental rights.

325 The NDPR is a partial reproduction of the EU GDPR with some modifications.

326 Charles D. Raab 'The Governance of Global issues: Protecting Privacy in Mathias Koenig–Archibugi and Michael Zurn (eds) *Personal Information in New Modes of Governance in the Global System* (Palgrave Macmillan, London, 2006.) 1.

including the Universal Declaration of Rights (UDHR), International Convention on Civil and Political Rights (ICCPR), the EU General Data Protection Regulation (GDPR) among others.[327] In Africa, a couple of treaties have also been adopted on data protection as discussed here under.

Universal Declaration on Human Rights (UDHR)

This was adopted in 1948 by the General Assembly of the United Nations as the first international document to identify human rights meant to be universally guaranteed by member states.[328] Unlike other international instruments with binding force, the UDHR was meant to provide a moral standard for member states on enforcement of fundamental human rights.[329]

In guaranteeing privacy, the UDHR provides that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[330]

To demonstrate the influence of UDHR on human rights in Nigeria, in 1995, the Federal Government set up the National Human Rights Commission to, among other Functions, deal with matters protecting human rights as guaranteed by the UDHR.[331] Right from the 1954 Constitution[332] up to the extant 1999 Constitution, provisions on privacy of citizens, homes, correspondences etc.

327 Rogers Clarke, 'International Instruments Relating to Privacy Law' < http://www.rogerclarke.com/DV/PLawsIntl.html > accessed 18 April 2021.
328 Alexandra Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyber space' (2014) 2(2) Groningen Journal of International Law, 34.
329 Jacob Dolinger, 'The Failure of the Universal Declaration of Human Rights' (2016) 47 University of Miami Inter American Law Review, 184.
330 Article 12.
331 Jacob A. Dada, 'Human Rights Protection in Nigeria: The Past, the Present and Goals for Role Actors for the Future' (2013) 14 Journal of Law, Policy and Globalization, 4.
332 The Nigeria (Constitution) Order in Council, 1954.

had been inspired by the UDHR[333] which lists privacy as one of the basic rights serving as standard for every nation in the world including Nigeria.[334] Some researchers have however argued that the UDHR has acquired a binding force owing to the consistent application of its principles by member states since its adoption as replication in successive national bills of rights.[335] Successive Nigerian Constitutions have in turn taken their lead from the UDHR by replicating provisions on privacy of citizens, homes and correspondences relying on the standards set by the declaration.

International Convention on Civil Political Rights (ICCPR)

In a reaction to the dictates of the UDHR, the ICCPR was adopted in 1966[336] as the third limb of the International Bills of Rights along with the International Covenant, Economic, Social and Cultural Rights (ICESCR) and the UDHR itself.[337]The ICCPR's main objective is the guarantee of a wide range of civil and political rights founded on the basic democratic values and freedoms for every human without discrimination as to race, gender, ethnic considerations etc.[338] In an identical manner with the UDHR, the ICCPR provides for right to privacy thus:

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful

333 Prior to the adoption of the declaration, the existing legal framework on privacy was not elaborate to cover most aspects of the concept. See Vivek Krishnamurthy, 'A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy' (2020) 114 AJIL Unbound, 26–30: Oliver Diggelman and Maria Nicole Cleis 'How the Rights to Privacy Became a Human Right' (2014) 14(3) Human Rights Law Review, 441.

334 Ani Comfort Chinyere 'Rudiments of Human Rights' (2016) 1(2010) Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 1.

335 Henry J. Steiner and Philip Alston, *International Human Rights in Context, Law Politics, Morals* (2nd ed Oxford University Press, 2000) 1; Hurst Hannum, The UDHR in National and international Law (1998) 3(2) Health and Human Rights, 149.

336 Von Christopher and N.J. Roberts 'William H.F. Fitzpatrick's Editorials on Human Rights (1994)' < https://www.geschichte–menschenrechte.de/schluesseltexte/william–h–fitzpatricks–editorials–on–human–rights–1949 > accessed 2 April 2021.

337 John P. Humphrey, 'The International Bills of Rights: Scope and Implementation' (1976) 17(3) William & Mary Law Review, 528.

338 Kristen D.A. Carpenter, 'The International Covenant a Civil and Political Rights: A Toothless Tiger' (2000) 26(1) North Carolina Journal of International Law and Commercial Regulation, 1.

attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attack." [339]

On the relationship of this provision with data protection, Bygrave argues that 'caselaw developed around article 17 of the ICCPR provides the clearest indication that the right to privacy in international law harbours core data protection principles. This is particularly significant as the ICCPR has the greatest reach of treaties on human rights, having been adopted by some two–thirds of the world's nation–states.'[340] In the same vein, Harland says, it is an 'expanded hard–law version' of the UDHR.[341]

Although Nigeria ratified the ICCPR in July 1993, prior to its ratification, right to privacy had existed in her preceding Constitutions[342] but while it is conceded that Nigeria's non–domestication of the ICCPR makes it unenforceable before her courts, the contents of the international treaty continue to influence the courts in their interpretation of Nigerian human rights laws. Nigeria practices a dualist system which requires international treaties to be re–enacted into law by the National Assembly before it can become enforceable in the country which practice was inherited from the English laws as noted by the Supreme Court in *Ibidapo v Lufthansa Airlines*[343]that "Nigeria, like any other commonwealth country, inherited the English Common law rules governing the municipal application of international law.[344]

339 International Covenant on Civil and Political Rights, article 17.
340 Lee A. Bygrave 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology, 247.
341 Christopher Harland, 'The Status of the International Covenant on Civil and Global Survey Through UN Human Rights Committee Documents' (2000) 22(1) Human Rights Quarterly, 187–260.
342 Jacob A. Dada, 'Human Rights Protection in Nigeria: The Past, the Present and Goals for Role Actors for the Future' (2013) 14 Journal of Law, Policy and Globalization, 1.
343 (1997) 4 NWLR (Pt. 498) 124 at 150.
344 See also Abacha v Fawehinmi (2000) 6 NWLR (Pt. 32) 811; Anthony O. Nwafor, 'Enforcing Fundamental Rights in Nigerian Courts–Processes and Challenges' (2009) 4 African Journal of Legal Studies, 1–11.

The Supplementary Act on personal data protection within the ECOWAS.

Supplementary Act A/SA. 1/01/10 was adopted in Abuja on the 11th day of February 2010 at the thirty–seventh session of the authority of Heads of state and government within the ECOWAS sub region.[345] The Act is drafted in a technology–neutral wording to set up a legal system governing the protection of personal data within the ECOWAS region with the objective of harmonizing the data protection laws of member states.[346]

By Nigeria's signing of the Act, she undertook to 'establish a legal framework for protection of data privacy relating to collection, processing, transmission, storage and use of personal data without prejudice to the general interest of the state'[347] and this Act remotely influenced Nigeria's legislative attempts towards enacting a principal data protection law.[348] The Act however suffers same fate as the ICCPR due to its non–domestication in Nigeria.[349]

General legislation

The Constitution of the Federal Republic of Nigeria, 1999 (as amended) ('1999 Constitution')

From whatever prism data protection is viewed, its origin is traceable to informational privacy guaranteed under the *Nigerian*

345 The signatories were: Benin, Burkina Faso, Cape Verde, Cote d'voire, Gambia, Guinea Bissau, Mali, Nigeria, Sierra leone and Togo.
346 Uchenna Jerome Orji, 'A Comparative Review of the ECOWAS Data Protection Act' (2016) 17(4) Computer Law Review International, 108.
347 Supplementary Act on personal data protection within the ECOWAS, article 2.
348 Olumide Babalola, 'A Bird's Eye Rundown on Nigeria's Data Protection Legal and Institutional Model' (2021) 12(2) Gravitas Review of Business & Property Law, 1.
349 Abba Amsami Elgujja, 'A Synopsis on Data Protection Under the Nigerian Laws: Has the Universality of Right to Privacy Tricked Down to Nigeria? (2020) < https://osf.io/fk5xg > accessed 12 April 2021.

Constitution.[350] Section 37 of same Constitution provides for privacy of citizens, homes, correspondence, etc and in 2014, the Court of Appeal in *Nwali v Ebonyi State Independent Electoral Commission (EBSIEC)*[351] interpreted the provision to include all aspects of human life. Although the court did not particularly use the phrase 'data protection' in the judgment, academics and practitioners have on the other hand, argued that the Nigerian Constitution is the foundation of all data protection provisions in Nigeria but this position is however suspect when it is considered that, while privacy under the Nigerian Constitution protects citizens, data protection on the other hand, universally, guarantees protection to residents. Conversely, since informational privacy contemplates data protection, then section 37 of the Constitution continues to provide a source for data protection in Nigeria until a principal substantive legislative is enacted on the subject. In a much recent decision in Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission (NIMC) (Unreported CA/IB/291/2020), the Court of Appeal on the 24th day of September 2021, emphatically held that data protection under the NDPR falls under section 37 of the 1999 Constitution.

The Nigeria Data Protection Regulation (NDPR) 2019.

In a historic move that set the tone for Nigeria's data protection landscape, the National Information Technology Development Agency (NITDA)–Nigeria's self–assigned national DPA, released the Nigeria Data Protection Regulation (NDPR) in 2019 to 'safeguard data privacy rights of natural persons, ensure a personal data during transaction are safely done, avert manipulation of personal data and ultimately ensure Nigeria business measure

350 The Constitution of the Federal Republic of Nigeria, 1999 (as amended) published in Gazette No. 27, Volume 83 of 5th day of May 1999.
351 (2014) LPELR 23682 (CA).

up to international data protection standards.'[352]

The NDPR in its extraterritorial scope, surprisingly applies to Nigerian citizens residing outside the country[353] but the propriety of this regulatory scope is not the focus of this article. The regulation, reportedly draws its inspiration from the GDPR, however it stands out with its creation of enforcement agents in the mould of Data Protection Compliance Organizations (DPCOs) which are licensed by the regulator to co–ensure compliance with the NDPR.[354] The regulation however suffers many inhibitions in terms of: uncertainty surrounding NITDA's statutory powers to regulate data protection; the extraterritoriality of its scope without parameters for enforcement; conflation of American and European concepts of data privacy with data protection and personal data with personal identifiable data; omission of legitimate interest as one of the basis of lawful processing; confusion of data administrator with data processor; recognition of multiple data protection authorities. etc.

Other General Legislation on Data Protection

Nigeria Police Act, 2020 was enacted to provide a framework for the police and ensure better cooperation with the host communities. While combating crime, this Act empowers the police to process personal data of persons arrested, store them on a retrievable format and honour data subjects' access request.[355] The absence of a particular data retention period could be interpreted to mean that the police force can store such information indefinitely as found in some other jurisdictions.[356]

352 NDPR, reg. 1(1)(a)–(d).
353 NDPR, reg. 1.2(b).
354 Diyoke Chika and Edeh Tochukwu, 'An Analysis of Data Protection and Compliance in Nigeria' (2020) 4(5) International Journal of Research and Innovation in Social Science, 377.
355 Sections 44, 46 and 68, Nigeria Police Act, 2020.
356 See section 9(1) of the English Protection of Freedoms Act, 2012 empowering the police to retain personal data for an indefinite period.

Federal Competition and Consumer Protection Act (FCCPA)[357] predominantly protects the interests of consumers by regulating business practices to ensure fair competition and qualitative services and goods. Although the Act does not include data protection in the consumer rights guaranteed,[358] it provides a retention period for records pertaining to certain data subjects and business operations.[359]

Companies and Allied Matters Act[360] regulates incorporation of companies, registration of business names and incorporation of trustees etc. and it as well empowers the statutory regulator–Corporate Affairs Commission–to protect and restrict access to personal information in certain cases in fulfilment of the data protection principle of integrity and confidentiality.[361] Under the Act, corporate bodies are mandated to retain electronic copies of official documents (which ordinarily contain personal data) for a period of six years.[362]

Child's Rights Act.[363] The prevalent violation of the rights and freedoms of children in Nigeria led to the enactment of this Act in 2003 to principally define the age of a child and protect his/her interests including right to privacy. The Child's Right Act guarantees protection of a child's personal data including information relating to his/her family life, home, correspondence, telephone conversations, communications subject to the right of

357 Published in Federal Government of Nigeria's Official Gazette, Government Notice No. 5, Vol. 106 on the 1st day of February 2019.
358 Ukwueze and Ibegbulem however alluded that the FCCPA does not contain any data protection provision without considering its provision on data retention. See Festus Okechukwu Ukwueze, Dike Justin Ibegbulem, 'Deconstructing Nigeria's Data Protection Regime from Consumer Protection Perspective' (2021) 13(1) Law, State and Telecommunications Review, 94–188.
359 Section 91 (1) and (2), FCCPA provides for indefinite retention of accounting records which may contain personal data.
360 Cap. A. No. 3 of 2020.
361 Section 324–329; See also the provisions of regulation 17 of the Companies Regulations 2021 made pursuant to section 867 of the Companies and Allied Matters Act.
362 Section 864, Companies and Allied Matters Act, 2020.
363 No. 26 of 2003.

supervision and control exercised by parents and legal guardians.[364]

Labour Act LFN 1990[365] is Nigeria's general law regulating employment and labour–related matters, but its application is however limited to 'workers' as opposed to employees.[366]It provides for retention of workers' personal data, record of wages, and conditions of employment for a minimum of three (3) years while recruiters have an indefinite period of data retention.[367]

National Archives Act[368] regulates the retention and storage of all kinds of records processed by private and public bodies in Nigeria by permanently preserving them for research purposes. The Act requires companies that have been in operation for over 25 years to establish archives division where records (including personal data) are stored indefinitely.[369]

The National Minimum Wage Act[370] prescribes a national minimum wage for Nigerian employees and legal framework for its seamless review. The Act requires employers to keep records of payment of wages or conditions of employment for three years[371] and this is also backed by the provision of section 75(2) of the Labour Act.

Employees Compensation Act[372] repealed the Workmen's Compensation Act 2004 by providing for a comprehensive recompense for employees who suffer occupational hazard in the course of employment. It requires records or documents at

364 Section 8(1) and (3), Child's Rights Act, 2003.
365 No. 21 of 1974.
366 Section 91 of the Labour Act defines the term 'worker' to exclude persons employed for administrative, executive, technical or professional purposes.
367 Sections 27(1)(7) and 75(1)–(3), Labour Act LFN 1990.
368 No. 12 1992.
369 Sections 8, 34 and 45, National Archives Act.
370 The Act repealed the 2004 Act by increasing the national minimum wage in 2019.
371 Section 10 (1), National Minimum Wage Act, 2019.
372 Cap. W6 of 2010.

the relevant workplace to be retained and left undisturbed for a reasonable period and to indefinitely keep records of payrolls.[373]

Personal Income Tax (Amendment) Act[374] regulates conditions for payment of income tax etc in Nigeria. Under the Act, employers are required to store and keep books of accounts relating to tax records of employees indefinitely.[375] Although the Act does not expressly state the contents of the books which are left to the discretion of the relevant tax authority, they may include general ledger, cash receipts, disbursement journal, sales journal etc which documents contain personal data.

Freedom of Information (FOI) Act.[376] In response to the rising level of Nigeria's corruption index, the FOI Act was enacted in 2011 to ease access to public information and records for transparency, accountability, and whistleblowing in governance. The Act however empowers a public body to prevent disclosure of public records containing personal data[377]where such disclosure will interfere with the data subject's privacy.[378]

National Identity Management Commission Act[379] governs Nigeria's national identity database and administration of citizens' identity management and maintenance system. The Act is Nigeria's most comprehensive legislative framework on national identity system with copious provisions dealing with data breach, integrity and confidentiality of personal data management.

373 Sections 39(9), 41 and 52, Employees Compensation Act, 2010.
374 No. 115, Vol. 98 published on 24th day of June 2011.
375 Section 12, Personal Income Tax (Amendment) Act, 2011.
376 No. 4 of 2011.
377 Sections 12(1) and 14(3), Freedom of Information (FOI) Act, 2011.
378 In the decision in (unreported) Suit no. FHC/L/CS/342/2019 between *Nlemoha v West African Examination Council (WAEC)* the court refused to grant access to a politician's WAEC examination certificate on the ground that it contained personal data, would interfere with his privacy, and that it fell under the exceptions provided in the Freedom of Information Act. See Olumide Babalola, *Casebook on Data Protection* (Noetico Repertum, Lagos, 2020) 97.
379 No. 23 of 2007.

It guarantees data security and protects unauthorized access to national database of Nigerians, with exceptions.[380]

Trafficking of Persons (Prohibition) Enforcement and Administration Act[381]establishes an agency responsible for the investigation and prosecution of human traffickers on one hand and the rehabilitation and counselling of trafficked persons on the other hand. Processing of victims' personal data is an integral part of the agency's performance of its statutory duties, hence the Act provides for some safeguards protecting the personal data and identities of victims and persons who volunteer information on human trafficking.[382]

Violence Against Persons Prohibition Act[383] prohibits all forms of violence against persons in public and private spheres by providing protection and remedies for victims of such dastardly acts. In judicial proceedings relating to domestic violence, highly sensitive information are often processed, hence, the enactment prevents disclosure of personal data of parties to the proceedings whether in relation to domestic violence or any other issue under the Act.[384]

Administration of Criminal Justice Act[385] procedurally governs criminal justice system in federal courts in Nigeria. In deserving cases, the identities and personal data of victims of crime and witnesses are protected from unauthorised access–they are not made public like other court–related information even though trials are meant to be conducted in public. The Act forbids the disclosure of victims' personal data on courts' records of

380 Section 26, National Identity Management Commission Act, 2007.
381 No. 4 of 2015.
382 Section 46, Trafficking of Persons (Prohibition) Enforcement and Administration Act 2015.
383 Entered force on the 25th day of May 2015.
384 Section 39(1), Violence Against Persons Prohibition Act, 2015.
385 Signed into law in May 2015.

proceedings in the prosecution of some offences.[386]

HIV and AIDS Anti–Discrimination Act[387] criminalises discrimination against persons diagnosed with HIV AIDS and precludes employers from conducting pre–employment HIV tests as a condition for employment. The Act prohibits the disclosure of the medical status of infected persons without their consent, guarantees anonymous testing on request and confidentiality of health data.[388]

National Health Act[389] provides a framework for the regulation, development, and management of heal systems and health services standards in Nigeria.[390] The Act guarantees information to data subjects on their medical records, retention of medical data for an indefinite period, confidentiality of data and non–disclosure of medical data to third parties, with exceptions.[391]

Cybercrime (Prohibition, Prevention etc) Act[392] provides institutional framework for combating cybercrime and promotion of cybersecurity but the legislation falls short of proper legal framework for cybersecurity in Nigeria. The Act criminalizes interception of personal data and mandates service providers to retain traffic data and subscribers' information for two years.[393]

Credit Reporting Act.[394] One of the objectives of this enactment

386 Section 232 (2), Administration of Criminal Justice Act 2015*:* See also Ogbonna Chukwumerije, 'Anonymous Court Proceedings, The Time is Now' (2021) < https://guardian.ng/features/law/anonymous–court–proceedings–the–time–is–now/> accessed 9 March 2021.
387 No. 7 of 2014.
388 Sections 10, 11, 12 and 13, HIV and AIDS Anti–Discrimination Act 2014.
389 No. 8 published in Vol. 101, number 145 of 27th day of October 2014.
390 The National Health Insurance Operational Guidelines (Revised) 2012 made pursuant to the National Health Insurance Act 1999, mandate certain employers to keep medical records belonging to employees and dependents. See paragraph 1.1.1 5 (d).
391 Sections 23, 25 and 26, National Health Act 2014.
392 2015.
393 Sections 12 and 38(1), Cybercrime (Prohibition, Prevention etc) Act 2015.
394 Enacted on the 20th day of May 2017.

is the promotion of access to accurate, fair and credible credit information as well the protection of the confidentiality of such information. The Act prescribes a retention period for debtors' records, right of access to personal data, confidentiality and integrity of personal data, data subjects' rights.[395]

Official Secrets Act[396] was enacted to predominantly protection state's secret, prevent and punish espionage. Although when this Act was enacted in 1962, data protection had not even taken off in Europe, however, its provisions are applicable to the modern–day data protection principle of integrity and confidentiality in that, it criminalizes the unauthorized disclosure and/or transmission of certain classified (personal) information.[397]

Money Laundering (Prohibition) Act[398] makes provisions prohibiting the financing of terrorism, the laundering of the proceeds of crime etc. The Act requires certain (financial) service providers to retain transaction records including customers' identities for a minimum of 10 years.[399]

Advance Fee Fraud and Other Fraud Related Offences Act 2006 combats advanced fee fraud *and* makes it a duty for data controllers providing electronic communication services to retain the personal data of customers and it also mandates Internet Service Providers (ISPs) to maintain a register of customers.[400]

395 Sections 5, 7, 9 and 10, Credit Reporting Act.
396 No. 29 of 1962.
397 Section 1, Official Secrets Act 1962.
398 No. 7 of 2003.
399 Sections 3(2), 7(a) and (b), Money Laundering (Prohibition) Act, 2003.
400 Sections 12 and 13, Advance Fee Fraud and Other Fraud Related Offences Act 2006.

Sector–specific (subsidiary) legislation[401]

Apart from the principal legislation with data protection provisions, some regulators have also issued certain regulations or guidelines wholly or partly for the protection of personal data in their various sectors pursuant to the relevant enabling legislation.

For lawyers and legal practice in Nigeria, *the Rules of Professional Conduct for Legal Practitioners 2007* made pursuant to Legal Practitioners Act[402] mandates lawyers while providing legal services or in the course of their employment, to ensure confidentiality of their clients' personal data in terms of security and unauthorised disclosure without the clients' consent within the context of professional privilege.[403] In the banking sector, the Central Bank of Nigeria has invoked its regulatory powers under the Central Bank of Nigeria Act[404] to issue a number of guidelines with data protection provisions to wit:

The *Guidelines on Mobile Money Services* was released in 2015 to 'ensure a structured and orderly development of mobile money services in Nigeria, with clear definition of various participants and their expected roles and responsibilities.' To achieve this, the guidelines require mobile money operators to retain records of transactions on their platform for a minimum of 7 years and ensure the confidentiality and privacy of customers.[405] *Guidelines on Transaction Switching Services 2016* was issued to develop electronic payment systems and transactions made thereunder, assign financial institutions the duty of confidentiality and

401 This list is not exhaustive as there exists other Nigerian sector–specific subsidiary rules with provisions on data processing (retention, transmission etc) too numerous and scattered to be capture here.
402 Cap 20, Laws of the Federation, 1990.
403 Rule 19, Rules of Professional Conduct for Legal Practitioners 2007.
404 See sections 2, 47 and 57, Central Bank of Nigeria Act, 2007 published in Gazette No. 55, Vol. 94 on the 1st day of June 2007.
405 See the preamble, clause 3.0(c), 14.1(c)(ii), 17.0 (e) and clause 1(9) of the appendix to the Guidelines on Mobile Money Services 2015.

integrity with respect to personal data obtained from customers while providing the services contemplated by the guidelines.[406]

In 2017, the *Regulatory Framework for Bank Verification Number Operations (BVN) Operations and Watchlist for the Nigerian Financial System* was released to ensure efficiency in bank customers identification for the enhancement of safe and seamless financial transactions by introducing the Bank Verification Numbers (BVN) stored in a database issued to all bank customers for identification purposes. The framework requires the custodians of the BVN database, and all parties involved in its processing to adopt (data) security measures and ensure confidentiality of bank customers' personal information.[407]

Regulatory Framework for use of USSD 2018 was issued to regulate the utility of technology to access mobile–based financial services including Short Messaging Service (SMS), Unstructured Supplementary Service Data (USSD), Interactive Voice Response (IVR), Wireless Application Protocol (WAP), stand–alone mobile application clients and SIM Tool Kit (STK). To ensure data security, the framework prescribes encryption of USSD by an auditable process[408] and radio encryption between users.[409] The *Risk–Based Cybersecurity Framework 2018* guides the Nigerian financial institutions on the 'minimum cybersecurity baseline' to be implemented and the requisite risk–based approach recommended for managing cybersecurity risks in financial transactions. It generally sets regulatory standards for financial institutions tasking them to take proactive measures to secure customers' personal data, to control access to such data and

406 Clauses 2.6.7 and 2.6.8, Guidelines on Transaction Switching Services 2016.
407 Clauses 1.6(viii), 1.13 (i)–(iv), Regulatory Framework for Bank Verification Number Operations (BVN) Operations and Watchlist for the Nigerian Financial System.
408 Clause 6.1, Regulatory Framework for use of USSD 2018.
409 Clause 6.4, Regulatory Framework for use of USSD 2018.

develop data breach management mechanisms.[410]

The *Consumer Protection Regulations 2019* was issued to provide minimum standards expected of financial institutions with respect to management and protection of customers' personal data processed during provision of financial services. The regulations were also issued pursuant to the provisions of Banks and Other Financial Institutions Act[411] to generally ensure privacy of bank services consumers by guaranteeing confidentiality of customers' information against unauthorized access and be accountable for such omission, and to seek and obtain consent before sharing with third parties etc.[412]

For the telecommunications sector, the Nigerian Communications Commission (NCC) also issued a number of regulations with data protection implications pursuant the enabling provision under the Nigerian Communications Act.[413]

The *Consumer Code of Practice Regulations*[414] was issued to define the procedure for the operations of telecommunication companies with respect to their relationship with telephone subscribers. The Code that was issued before the NDPR requires telecommunication companies to observe the kind of principles of data processing now recognised under the EU GDPR. [415]

Registration of Telephone Subscribers Regulations[416] was issued in 2011 as a regulatory framework to register, control and manage the database of GSM mobile telephone line subscribers in Nigeria.

410 Clause 3, Risk–Based Cybersecurity Framework 2018.
411 Section 57, Banks and Other Financial Institutions Act, Laws of the Federation 2010.
412 Clause 5.4.1–5.4.6, Consumer Protection Regulations 2019.
413 Section 70, Nigerian Communications Act published in Government Notice 115, Number 62, Volume 90 on the 19th day of August 2003.
414 Published in Government Notice 56, Number 87, Volume 94 on 10 July 2007.
415 Section 35(1) and 57, NCC Consumer Code of Practice Regulations. The provision also guards against data breach–accidental disclosure.
416 Published in Government Notice 229, Number 101, Vol. 98 on the 7th day of November 2011.

The regulations expressly recognise data subjects' privacy, their right of access to personal, right to rectification of data as well as some data retention provisions, etc.[417]

The *Internet Code of Practice* was released in 2019 to relevantly provide for telecommunication companies' obligations on the protection of subscribers' personal data in their custody. The Code also regulates activities of ISPs with provisions on transparency, data security and breach notification procedure[418]

Nigerian Communications (Enforcement Process etc) Regulations[419] was issued to provide the procedural rules and framework for enforcing the Nigerian Communications Act. The regulations, among other obligations, mandate telecommunication companies to retain call or traffic data[420] for two years.[421]

For the ICT sector, NITDA issued *Guidelines for Nigerian Content Development in Information and Communication Technology (ICT)*[422] in 2013 to, among other objectives, to localize and increase indigenous production, sales and consumption of ICT products and services for the Nigerian market. To achieve this objective, the guidelines mandate data and information management Firms to adopt data security measures and to localise data.[423]

417 Regulation 9(1) and (4), NCC Registration of Telephone Subscribers Regulations.
418 Clauses 3.1 and 4, NCC Internet Code of Practice.
419 Published in Notice 22, Number 11, Volume 106 on the 22nd day of January 2019.
420 The ICO defines traffic data as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication' See Information Commissioner's Office, 'Traffic Data' https://ico.org.uk/for–organisations/guide–to–pecr/communications–networks–and–services/traffic–data/ accessed 22 August 2021.
421 Regulation 8(1), Nigerian Communications (Enforcement Process etc) Regulations 2019.
422 Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) was issued by NITDA under the auspices of the Federal Ministry of Communications.
423 Clause 14.0, Guidelines for Nigerian Content Development in Information and Communication Technology (ICT).

CHAPTER EIGHT

Relationship between data protection and other rights

Whether it is enjoyed as a component of privacy or exercised as an autonomous and separate right,[424] the concept of data protection ought to be defined and understood at the very least in terms of its interplay with other rights and freedoms. Neither privacy nor data protection is recognized under the African Charter on Human and Peoples Rights, but with a semblance of right to respect for family life, it obliges member states to assist the family as custodian of morals and traditional values recognized by the community.[425] However, the African Union (AU) appears to have however retraced it steps by the adoption of the Convention on Cybersecurity and Personal Data Protection (Malabo Convention) mandating member states to establish legal frameworks regulating data protection and free flow of data within the continent but this treaty is not yet enforceable as a result of the provision in article 36 which makes it enforceable only upon ratification by 15 member states.[426]

424 Data protection is a stand–alone right under article 8 of the Charter of Fundamental Right of EU and article 16 of the Treaty in the functioning of the European Union (Lisbon Treaty). See Yvonne McDermott, 'Conceptualizing the Right to Data Protection in the Era of Big Data' (2017) Big Data and Society, 1–7.

425 African Charter on Human and Peoples Rights (Canjul Convention), art. 18(1) and (2). See also Obinna Okere 'The Protection of Human Right: A comparative Analysis with the European and American Systems' (1984) 6(2) Human Rights Quarterly, 141–159.

426 As of June 2021, only fourteen states had ratified namely: Benin, Sierra Leone, Congo, Ghana, Guinea Bissau, Mozambique, Mauritania, Rwanda, Chad, Suo Tome and Pimipe, Togo, Tunisia, and Zambia. See African Union, 'List of Countries that have ratified/acceded to the African Union Convention on Cybersecurity and Personal Data Protection' < https://au.int/sites/default/files/treaties/29560–sl–AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> accessed 12 April 2021.

Unlike in Europe where a number of international and municipal legal instruments recognize data protection as a distinct right from the right to privacy,[427] it does not enjoy such luxury in Africa. Apart from the Treaty on the Functioning of the Functioning of the European Union, (TFEU) the European Union Charter of Fundamental Rights (EUCFR) also guarantees right to data protection,[428] the existence of which right has also been confirmed by the Court of Justice of the European Union (CJEU) in a number of cases where the right to protection of personal data was judicially emphasised.[429] It has however been noted that, apart from its creation under the charter, there exists no fundamental right to data protection under the ECHR, hence scholars have queried the legal force of the charter in relation to fundamental right as against the ECHR.[430] However, although data protection is not yet a distinct fundamental right in Nigeria, it is conceivable under informational privacy guaranteed by section 37 of the 1999 Constitution and this much is acknowledged under one of NDPR's objective that seeks to safeguard the rights of natural persons to data privacy.[431] Nevertheless, while data protection does not stand alone under the extant 1999 Constitution, it overlaps with a number of other related but distinct rights.

427 Art. 16 of Treaty on the Functioning Rights of European Union provides that: Everyone has a right to the protection of personal data concerning them. The provision does not only effectively create a data protection right in the EU but it also empowers individuals to approach the courts and ventilate issues on violation of such right. See Daniel Cooper, Henriette Tidemans and David Fark, 'The Lisbon Treaty and Data Protection: what next for Europe's Privacy Rules?' < https://www.cov.com/–/media/files/corporate/publications/2010/02/the–lisbon–treaty–and–data–protection–whats–next–for–europes–privacy–rules.pdf > accessed 13 April 2021, Hielke Hijmans and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?' (2009) 46(5) Common Market Law Review, 1.

428 See article 8(1) and (2), European Union Charter of Fundamental Rights.

429 See Promusicae v Telefonica de Espana, C–275/06 and Tietosuojavaltuutetta v Satakunnan Markkinaporssi Oy, Satamadin Oy, C–73/07.

430 Gloria G. Fuster and Raphael Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' (2012) 26(1) International Review of Law, Computers & Technology, 73–82 and Gloria G. Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU' (2005) 52(4) Common Market Law Review, 1139–1142. The General Data Protection Regulation also recognizes data protection as fundamental right, see art. 1(1) and (2); Maria Tzanou, *The Fundamental Right to Data Protection Normative Value in the Context of Counter–Terrorism Surveillance* (Hart Publishing, Oxford, 2017) 12.

431 NDPR, reg.1.1(a).

Data Protection and Right to Privacy

These are twin concepts used interchangeably and they frequently overlap since they have similar objectives and purpose; hence they are often used synonymously. While the right to privacy does not necessarily protect all information that can identify a natural person, that is what data protection secures.[432] In conceptualizing their interplay, both notions have been argued to perform same fundamental roles but while privacy is regarded as a 'tool of opacity' providing checks and control over unjustifiable intrusion into an individual's private spaces, data protection is a 'tool of transparency' which sets the boundaries and instructions for processing of personal data with an extensive definition as opposed to private life.[433]

In offering protection for individuals, each concept ought not to work in isolation, one does not exclude the other, they are complimentary in their operation, hence, privacy offers substantive protection while data protection provides the procedural guidelines to maximize such protection.[434] On the concepts' interdependence, Forde concludes that, 'data protection will always be dependent upon and ultimately collapse into privacy: data protection is denigrated to rules detailing requirements for consent and legitimate processing of information. As a 'transparency tool',

---

432 For a comprehensive reading on distinction between both concepts in Europe, see Juliane Kokott and Christoph Sobotta 'The Distinction between Privacy and Data Protection in Jurisprudence of the CJEU and the ECHR' (2013) 3(4) International Data Privacy Law, 222; Menno Mostert et al, 'From Privacy to Data Protection in the EU: Implications for Big Health Research' (2018) 25 European Journal of Health Law, 43–55; Adekemi Omotubora and Subhajit Basu 'Next Generation Privacy' (2020) 29(2) Information & Communications Technology Law, 151–173.

433 Paul de Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Serge Gutwirth, Anthony Duff and Erik Claes (eds) *Privacy and the Criminal Law* (Intersentia, Cambridge, 2006.) 1.

434 Norbeto Nuno Gomes de Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer–Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds) *Privacy and Identity Management for life* (1st edn, Springer International Publishing, New York, 2011) 96; Federico Ferretti, *EU Competition Law, the Consumer Interest and Data Protection: The Exchange of Consumer Information in the Retail Financial Sector* (Springer International Publishing, New York, 2014) 105.

data protection rules serve to assist in the realization of privacy.'[435]

Irrespective of their differences as two sides of the same coin, the twin concepts interact in many ways all for the protection of private sphere especially when data protection is considered as an offshoot of privacy. In analysing the relationship between the two concepts, Tzanou says 'data protection appeared an offspring of privacy and the two rights still seem inextricably tied up together with a birth cord. However, as a child data protection is trying to mark its own way in life.'[436]

Researchers are however torn between two schools of thought: the reductionists and the coherent/non–reductionists. The former argues that data protection ought to be exercised as a stand–alone fundamental right completely detached from privacy[437] and that data protection guarantees others fundamental norms other than privacy, hence, restricting it to privacy could deprive the society from deriving other benefits from it.[438] Privacy is noted to guarantee less rights than data protection under which data subjects can exercise a wide variety of rights over their personal data, for instance, data subjects can restrict further processing of their personal data while taking a decision on whether to rectify same or outrightly object to further processing. [439]

On the flip side, the non–reductionists argue that data protection

435 Aidan Forde, 'The Conceptual Relationship Between Privacy and Data Protection' (2016) 1 Cambridge Law Review, 140.

436 Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? (2013) 3(2) International Data Privacy Law, 88–99.

437 See Nicholas Scandamis Frantzis Sigalas and Sofoklis Stratakis, 'Rival Freedoms in Terms of Security the Case of Data Protection and the Criteria of Connexity (2007) CEPS, Challenge, Research Paper No.7, 15; Gloria Gonzales Fuster, Paul de Hert and Serge Gutwirth, 'The Law–Security Nexus in Europe: State of the Art Report' (2008) Report submitted in fulfilment of Requirements of the FP7 Project Converging and Conflicting Ethical Values in the International Security Continuum in Europe (INEX) WPZ D21, 11.

438 See also Lee A. Bygrave, 'The Place of Privacy in Data Protection Law' (2001) University of New South Wales Law Journal, 241.

439 Orla Lynskey, 'Deconstructing Data Protection; The Added Value of a Right to Data Protection in the EU Legal Order' (2015)63 International & Comparative Law Quarterly, 590; Collete Cuijpers, 'A Private Law Approach to Privacy: Mandatory Law Obliged' (2007)4/4 SCRIPT ed 304–18 at 312.

has its origins in privacy, hence it cannot be completely severed from such right in other words, they are Siamese twins with slight differences but inseparable[440] but Makulilo aggregates the opposing views and concludes that: 'privacy and data protection are overlapping but distinct and separate concepts, they are synonymous and used interchangeably and their use must be contextualised to avoid confusion.'[441] While it is conceded that one of the distinguishing features of both concepts is that an information may be personal but not private.[442] Within the context of the Nigerian Constitution, data protection is inseparable from privacy when the meaning and purpose of both concepts are re–considered. In the light of the fragments in section 37 of the Constitution which guarantees 'privacy of citizens, their homes, communications etc (all these constitute personal data), one cannot discuss data protection in Nigeria without touching on privacy and this confirms their somewhat inseparability especially since the Court of Appeal has interpreted 'privacy of citizen' to be elastic enough to include his personal data (body, life, person, thoughts, belief, conscience, feelings, views decisions, including his plans and choices, desires, health, relationships, character, material possession, family life, activities.' [443] The expansive definition of 'privacy of citizens' under the 1999 constitution gives credence to a position that data protection is clearly situated in the relevant section. The European Court has rightly ruled that data protection is fundamentally important to an individual's exercise of his right to privacy thereby emphasising the conjoined

440 Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2007) 1; (Paul de Hert and Eric Schruders, 'The Relevance of Convention 108' 33, 42 Proceedings of the Council of Europe Conference on Data Protection, Warsaw November 19–20, 2001.

441 Alex B. Makulilo, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law, 165.

442 Christopher Docksey, 'Four Fundamental Rights: Finding the Balance' (2016) 6(3) International Data Privacy Law, 202.

443 See Nwali v Ebonyi State Independent Electoral Commission (2014) LPELR–23682 (CA).

nature of both concepts.[444] While the asymmetry between the two concepts are undeniable, on the current state of Nigerian law, the preferred view is that, data protection is not distinct from the right to privacy contemplated under the Nigerian Constitution otherwise the wind would be taken out of its sail as a fundamental right, hence it is bereft of the status bestowed on the such classes of rights.[445]

Data Protection and Freedom of Expression/Freedom of Information.

Freedom of expression interplays with and sometimes compliments data protection i.e an interference with the exercise of freedom of speech may also constitute an infringement on data protection rights. In *Digital Rights Ireland's* case, the ECtHR held that the storage of an individual's communications violated his data protection rights[446] and in similar circumstances, mass surveillance of communication without lawful basis violates freedom of expression and right to receive information on one hand, while it also constitutes interference with privacy of correspondence and data protection on the other.[447]

In some other instances, data protection could be at loggerheads with freedom of expression and this plays out in situations where an individual seeks to protect certain personal information from unauthorized disclosure but another entity or individual desires access to such information for various purposes since freedom

444 See Olumide Babalola, Casebook on Data Protection (Noetico Repertum, Lagos, 2020) 355; Z v Finland, no. 2209/93 ECHR 1997, Digital Rights Ireland and Seitlinger, (Joined) C. 293/12 and C. 594/12; Gonzalez Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the European Union (Springer, 2014) 1.
445 Fundamental Rights stand above ordinary laws of the land. Ransome–Kuti v Attorney General of the Federation (1985) 2 NWLR (Pt. 6) 211.
446 See Olumide Babalola, *Casebook on Data Protection* (Noetico Repertum, Lagos, 2020) 179.
447 Christopher Docksey 'Four Fundamental Rights: Funding the Balance' (2016) 6(3) International Data Privacy Law, 263; Sarah Matos, 'Privacy and Data Protection in the Surveillance Society: The Case of the Prüm System' (2019) 66 Journal of Forensic and Legal Medicine, 155–169.

of expression also includes right to receive information.[448] In resolving the conundrum, the courts have had to balance such competing rights against each other in deserving cases in favour of the weightier interest.[449]When determining which of the rights will prevail, the courts ought to consider every case on its own merit within the context of the extant and relevant constitutional provisions.[450]

In *Google Spain's* case, Costeja Gonzales asked Google to respect his data protection 'right to be forgotten' and de–reference a news item on social security debts because the information was outdated and no longer relevant, but Google argued that such request would interfere with the public's right to information and freedom of expression[451] but the court noted that the public's right to such information outweighed Gonzales' right by virtue of his status as a public figure.

Ultimately, freedom of expression guarantees the right to freely transmit and share ideas and opinions, but data protection regulates the transmission (processing) of such information where they relate to an identifiable human being.[452]

Data Protection and Right to Human Dignity

Floridi says human dignity is the foundation upon which right to privacy was founded. He further argued that 'the protection of privacy should be based directly on the protection of human dignity, not indirectly, through other rights such as that to property

448 Section 39 of the 1999 Constitution guarantees the right to receive information without interference.
449 Magdalene Jozwiak, 'Balancing the Rights to Data Protection and Freedom of Expression and Information by the Court of Justice of the European Union' (2016) 23(3) MJ, 404.
450 Stefan Kulk and Frederik Zuiderreen Borgesius 'Privacy of Expression and Right to be Forgotten in Europe' (2017) in Evan Selinger, Jules Polonetsky, Omer Tene (eds) *Cambridge Handbook of Consumer Privacy* (Cambridge University Press, Cambridge, 2018) 1.
451 Case C–131/12, 490.
452 Andres Calderon, Susana Gonzales and Alejandra Ruiz, 'Privacy, Personal Data Protection and Freedom of Expression Under Quarantine? The Peruvian Experience' (2021) 00(0) International Data Privacy Law, 11.

or to freedom of expression. In other words, privacy should be grafted as a first order–breach to the trunk of human dignity not to some of its branches, as if it were a second order right.'[453]

Data protection and human dignity may not however be mutually exclusive especially when their definitions are juxtaposed[454] but privacy, working together with right to dignity, is the core of fundamental and personality rights.[455]

Data Protection and Intellectual Property Rights

Personal data processed and stored in database for business purposes constitute trade secrets in which a data subject may claim intellectual property and proprietary rights[456] even though it is contentious to argue that data subjects own intellectual property rights in their personal data[457] distinguishable from the general property rights over personal data which remains jurisprudentially unsettled.[458] In *Coogan v News Group Newspaper Ltd,*[459] the Court of Appeal of England and Wales held that, confidential personal information is intellectual property and the court equated personal information having commercial value with intellectual property conferring the data subjects with a measure of control over the use of such information.

In the American case of *Price v Hal Roach Studios*[460]*,* the parties

453 Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philos. Technol, 307–312.
454 Anne de Hingh, 'Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation' (2018) 19(5) German Law Journal, 1270.
455 Cleber Sanfelici and Lucimare Plaza Tena, 'The Reasons that Justify the Rights of Privacy: Human Dignity as the Core of Personality Rights and Situations at Density that Allow Flexibility' (2016) 11(2) DOAJ, 476–498.
456 Jerome Richman and Pamela Samuelson 'Intellectual Property Rights in Data?' (1997) 50 Vand. L. Rev. 51.
457 Leon Trakman Robert Walters and Bruno Zeller, 'Is Privacy and Personal Data Set to Become the New Intellectual Property? (2019) International Review of Intellectual Property and Competition Law, UNSWLR, 70.
458 See Ivan Stephanov, 'Introducing a Property Right Over Data in the EU: The Data Producer's Right–An Evaluation' (2019) 34(1) International Review Law, Computers and Technology, 65.
459 (2012) EWCA civ 48, (2012)2 WLR 84 (2012) EMLR 14.
460 400 F. Supp 836. (S.D.N.Y. 1975).

disputed the use of names and likeness of two famous dead comedians. The relevant part of the decision was to the effect that, a person's name is his personal data over which he/she has a property right worthy of legal protection and the court concluded that an individual had inalienable property right in his name and could waive right to privacy over such in certain circumstances.

The current reality which sees the biggest businesses in the world thriving off people's personal data lends support to the argument that data subjects be allowed proprietary control over their personal information which has become more economically valuable than ever.[461]

While the traditional position of individual property law was that certain information (of generic or obvious nature) cannot be exclusively owned by a person, such is arguable and not always tenable under data protection law.[462] Conclusively, as an intellectual property, personal data could be "propertized" and individuals can make informed decisions on who to sell to and how to recoup compensation for their personal data in which they retain intellectual property rights.[463]

461 Of the ten most valuable companies in the world as at 2021, nine of them predominantly rely on technology and consumers' personal data for business sustenance, i.e. Apple, Microsoft, Amazon, Delta Electronics, Alphabet Inc., Tesla, Facebook, and Ali Baba Group.
462 Yochai Benkler, 'Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information' (1999) 15 Berkeley Tech Law Journal, 1.
463 Pamela Samuelson, 'Privacy as Intellectual Property' (2000) 52(5) Stanford Law Review, 1125–1173.

CHAPTER NINE

Scope and application of the NDPR

As gleaned from its preamble, the NDPR (the regulation) was issued in appreciation of the emerging data protection guidance within the international community and the need to secure lives and properties and commercial integrity within the Nigerian vulnerable data economy.

The regulation was issued as a subsidiary legislation on the 25th day of January 2019 by the National Information Technology Development Agency (NITDA) to regulate data processing activities involving Nigerians and residents of Nigeria. In terms of its scope and application, the regulation seeks to: (a) regulate manual and electronic processing of personal data;[464] (b) apply to residents or citizens of Nigeria within and outside Nigeria;[465] (c) protect data privacy rights guaranteed by Nigerian and foreign laws.[466]

Manual and electronic processing of personal data

The regulation is a bit contradictory when its scope on processing activities is considered together with its preamble which ought to provide some clarity on the piece of legislation. This contradiction is further confirmed when the regulation's scope is juxtaposed

464 NDPR, reg.1.2(a).
465 NDPR, reg.1.2(b).
466 NDPR, reg.1.2(c).

with the provision of the parent legislation–National Information Technology Development Agency Act (the Act)[467]with respect to NITDA's powers.

For the avoidance of doubt, the NDPR regulates both manual and electronic processing of personal data but in its preamble, it acknowledges that NITDA is only statutorily empowered to develop regulations for electronic governance (e–governance) and monitor the use of electronic data exchange[468] but under its scope, the NDPR purports to regulate 'processing of personal data notwithstanding the means by which the data processing is being conducted.'[469] In *Osadebay v Attorney General of Bendel State,*[470] the Supreme Court observed that an enabling or parent legislation gives validity to the subsidiary legislation, hence NITDA's regulation of manual processing is ultra vires its enabling Act. Also, in *Governor of Oyo State v Folayan*[471] that a subsidiary legislation deserves its validity and authority from a substantive law and it lacks the capacity to extend such authority.

Extra territorial scope

The regulation is applicable to Nigerian residents on one hand and Nigerians residing outside the country on the other hand[472] with the implication that the NDPR has extra territorial reach outside the shores of Nigeria. The term 'extraterritoriality' within the context of data protection has been defined as 'the exercise of jurisdiction by a state over activities occurring outside its borders.'[473]

467 Act No. 28 published in the Official Gazette No. 99 Volume 94 on the 5th day of October 2007.
468 Section 6 (a) and (c) only empower the agency to make guidelines for electronic exchange.
469 NDPR, reg. 1.2(a)
470 (1991) LPELR–2781 (SC).
471 (1995) LPELR–3179 (SC).
472 NDPR, reg. 1.2(b).
473 See Deborah Senz and Hilary Charlesworth, 'Building Blocks: Australia's Response to Foreign Extraterritorial Legislation' (2000) 2 Melbourne Journal of International Law, 69, 72.

As far as data protection laws are concerned, there are direct and indirect provisions on extraterritoriality; direct extraterritoriality will come into play where a controller carries on business in a country irrespective of whether it is incorporated is such country while indirect extraterritoriality refers to the collection of personal data of residents of a particular country even when the controller does not do business or have any business presence in that country.[474]

The extraterritoriality of the NDPR is somewhat peculiar in that, it focuses on the data subjects, rather than the controller contrary to the regular extraterritoriality clauses in other jurisdictions. For example, the English Data Protection Act 2018 references the GDPR for its scope of application and article 3 of the GDPR applies to controllers: (i) processing done by an entity in the union, (ii) processing of personal data of data subjects in the union (iii) monitoring of data subjects in the union (iv) processing by entities in a place where member state law applies.[475]

The NDPR does not only assume jurisdiction over data subjects and processing activities in Nigeria but also assigns jurisdiction to itself over data subjects outside Nigeria irrespective of the location of the controller or the applicable law and such provisions have been observed by notable scholars on the subject as a problematic 'regulatory overreaching.'[476] However, on the justification of extraterritoriality in data protection, Svantesson argues that:

'...this important quote highlights two reasons why 'extraterritorial

474 See Australian Privacy Act, 1988, section 5B and Singaporean Personal Data Protection Act, 2012, article 2(1); Dan Jerker B. Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot' Undermining the Regulation' (2015) International Data Privacy Law 5(4), 226, see also Google Spain's case which affirmed the exercise of a data subject's right beyond EU territory, Olumide Babalola, Casebook on Data Protection (Noetico Repertum, Lagos, 2020) 490.

475 GDPR, art. 3(1), (2) and (3); see also Cedric Ryngaert and Mistale Taylor 'The GDPR as Global Data Protection Regulation' (2020) 114 AJIL Unbound, 5.

476 Lee A. Bygrave, 'European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation' (2000) 16(4) Computer Law & Security Review, 252–257.

claims are made despite the potential enforcement difficulties. First, there is the mentioned symbolic value in showing an attempt at treating domestic and foreign organisations equally. And second, the claim of an extraterritorial effect may have a deterrent effect, at least if we assume that companies generally prefer not to violate any laws.'[477]

In the NDPR's case, its attempt at regulating citizens outside Nigeria without qualification is not only problematic, but it may also be totally unenforceable for two reasons:

First, the parent legislation lacks extraterritoriality provisions, hence the NDPR which is subordinate to it cannot unilaterally enlarge its own reach beyond that of its principal legislation especially since the Supreme Court once clarified that a subsidiary legislation does not have a wider binding effect or force than its paramount law.[478] For the avoidance of doubt, the functions, and powers of NITDA as donated by its enabling Act limit its activities within the shores of Nigeria and nothing therein confers jurisdiction on the agency to act outside the country.

Secondly, unlike other data protection laws that focus on controllers in their extraterritorial applications, the NDPR focuses on Nigerian citizens outside the country who are automatically outside the geographical jurisdiction of our laws and therefore consequently lack legal protection under Nigerian laws with exceptions. In the event of litigation, a decision on applicable law becomes problematic and raises questions on whether the provisions of the NDPR (a subsidiary legislation) can be invoked in foreign courts leading to issues of conflicts of laws.[479]

477 Dan Jerker Svantesson–Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5(4) International Data Privacy Law, 233.
478 See Osadebay v Attorney General of Bendel State (1991) LPELR–2781 (SC).
479 Maja Barka 'Data Protection and Conflict of Laws: A Challenging Relationship' (2016) 2(3) European Data Protection Law Review, 324–341.

Conclusively, since the NDPR is neither a statute nor an international treaty that is transposable and enforceable in foreign courts, it species of extraterritorial, to the extent of its proposal of protection for Nigerian citizens outside the country, is rather cosmetic and ought to be reviewed.

CHAPTER TEN

Definitions

A striking feature of data protection laws is the use of peculiar terms and terminologies with technical meanings and unusual implications. This chapter explores the definitions of the regular concepts and terms employed in the NDPR and the ones omitted in the regulation for proper understanding of the subject of data protection.[480]

'Consent' is 'any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'[481] 'Data' means 'characters, symbols and binary on which operations are

480 Some regular terminologies and concepts are omitted in the NDPR, hence resort is made to the GDPR for their meaning as follows: 'Profiling' is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. See art. 4(4) GDPR. 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. See art. 4(5) GDPR. 'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. See art. 4(13) GDPR. 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physio logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. See art. 4(1) GDPR. 'Binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. (art. 4(2) GDPR.

481 NDPR, reg.1.3(iii).

performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.[482] 'Database' is a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type databases.'[483] 'Data administrator' is 'a person or an organization that processes data.'[484]

'Data controller' is a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed.[485] 'Data processor' is 'any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).'[486] The GDPR defines it as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[487]

'Data portability' is 'the ability for data to be transferred easily from one IT system or computer to another through a safe and secured means in a standard format.'[488] Data protection means the 'preservation of a natural person from the misuse of his or her personal information.'[489] 'Data Protection Compliance Organization' (DPCO) is any entity duly licensed by NITDA (or any subsequent law) for the purpose of training, auditing,

482 NDPR, reg. 1.3(iv).
483 NDPR, reg. 1.3(viii).
484 This is an unjustifiable creation of the NDPR. Not only is there no known data protection legislation in the world where the term is found, the concept is not even used anywhere in the regulation apart from the definition. It is suspected that what is meant here is 'processor' as found twice in the body of the regulation.
485 NDPR, reg. 1.3(x).
486 The NDPR does not define this, but it is used in the body of the regulation. See English Data Protection Act 218, s. 32(3) and 83(3).
487 GDPR, art.4(8).
488 NDPR, reg. 1.3(xii).
489 This term is neither defined by the NDPR nor other data protection laws, but researchers have attempted its definition which is not as problematic as that of privacy. See Nicola Fabiano, 'Ethics and the Protection of Personal Data' (2019) Conference Paper at the 10th International Multi–Conference on Complexity, Informatics and Cybernetics, Florida, USA.

consulting, and rendering services and products for the purpose of compliance with the NDPR or any foreign data protection law or regulation having effect in Nigeria.'[490] Data subject refers to any person who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'[491] Data Subject 'Access request' is the mechanism for an individual to request a copy of their data under a formal process which may include payment of a fee.[492] Filing system is any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.[493]

'Personal data' is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.'[494]

'Personal identifiable information' (PII) means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual

490 NDPR, reg. 1.3(xiii).
491 Reg. 1.3(xiv).
492 Reg. 1.3(xv).
493 Reg. 1.3(xvi).
494 Reg. 1.3(xix).

in a context.[495]'Processing' is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[496] 'Personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[497] 'Recipient 'is a natural or legal person, public authority who accepts data.[498] 'Relevant Authorities' under the NDPR means the NITDA or any other statutory body or establishment having government's mandate to deal solely or partly with matters relating to personal data.[499]'Sensitive personal data' refers to data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.[500] Third Party is any natural or legal person, public authority, establishment or

495 Reg. 1.3(xx). In an attempt at defining PII, Schwartz and Solove say 'PII is a challenging conceptual issue at the heart of any system of regulating privacy in the information age. If PII is defined too narrowly, then it will fail to protect privacy in the light of modern technologies involving data mining and behavioural marketing. Technology will thus make privacy law irrelevant and obsolete. On the other hand, if PII is defined too broadly, then it could encompass too much information, and threaten to transform privacy law into a cumbersome and unworkable regulation of nearly all information. Privacy law must have coherent boundaries, which adequately protect privacy, and which can be flexible and evolving.' See Paul M. Schwartz and Daniel Solove, 'The PII Problem: Privacy and A New Concept of Personally Identifiable Information' (2001) 86 New York University Law Review, 1816. 'PII' is however an American concept while 'personal data' is a European concept. See Paul M. Schwartz and Daniel Solove, 'Reconciling Personal Information in the United States and European Union' (2014) 102(4) California Law Review, 877–916.

496 Reg. 1.3(xxi).

497 Reg. 1.3(xxii).

498 Reg. 1.3(xxiii). This definition is not however comprehensive enough to avoid confusion of 'recipient' with other entities that receive or accept data e.g. the processor or public authorities. For example, the English Data Protection Act defines 'recipient' as 'any person to whom the data is disclosed, whether a third party or not, but it does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law.' See section 33(5); The GDPR is also explicit enough to include public authorities in its own definition, see art. 4(9) GDPR.

499 NDPR, reg. 1.3(xxiv). By this definition, the regulation does not recognise NITDA as the exclusive or sole supervisory authority and this casts a doubt on its status as Nigeria's Data Protection Authority since that role resides in all public bodies that process data, and this list is almost endless in Nigeria. See also the provision of reg. 3.1(7)(j) NDPR that guarantees the right to lodge complaint with the 'relevant authority.'

500 NDPR, reg. 1.3(xxv).

any other body other than the data subject, the data controller, the data administrator and the persons who are engaged by the data controller or the data administrator to process personal data.[501]

Most of the definitions adopted in the NDPR are verbatim (or with slight modifications) reproductions of the definitions in the GDPR thereby giving further credence to the submission that European law is part of the source of data protection in Nigeria.

501 NDPR, reg. 1.3(xxvii).

CHAPTER ELEVEN

Principles of data protection

Notwithstanding the divergence of thoughts and perspectives plaguing the concept of data protection, scholars and researchers appear to be at one, on the principles governing the subject with slight variations here and there. Regardless of the argument around its nature, data protection is generally regulated by a number of universally acceptable principles[502] which were initially referred to as 'Fair Information Practices (FIPs) developed in a 1973 report by the Department of Health, Education & Welfare but the Organisation for Economic Cooperation and Development (OECD) revised it in its 1980 Guidelines and made it internationally embraced.[503] The Guidelines recognized eight principles thus: (i) collection limitation principle (ii) data quality principle (iii) purpose specification principle (iv) use limitation principle (v) security safeguards principle (vi) openness principle (vii) individual participation principle and (viii) accountability principle.[504]

502 The GDPR refers to them as principle of data processing in article 5 while the English Data Protection Act 2018 styles them as 'principles of data protection' in section 34(1).

503 See Robert Gellman, Fair Information Practices; A Basic History' (2021) <https://bobgellman.com/rg–docs/rg–FIPShistory.pdf> accessed 6 May 2021; Fred H. Cate, Peter Cullen, Victor Mayer–Schonberger, 'Data Protection Principles for the 21st Century, Revising the 1980 OECD Guidelines' (2014) <https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf> accessed 6 May 2021; Michael Kirby, 'The History, Achievement and Future of 1980 OECD Guidelines on Privacy' (2011)1(1) International Data Privacy Law, 6.

504 See Organisation for Economic Cooperation and Development, 'Thirty Years After: The OECD Privacy Guidelines' (2011) <https://bit.ly/3CqYs94> accessed 10 May 2021; OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 6 May 2021.

The principles have however been modified, developed and refined over time into seven core principles adopted by most contemporary data protection laws as seen in the EU GDPR thus: (a) lawfulness, fairness and transparency (b) purpose limitation (c) data minimization (d) accuracy (e) storage limitation (f) integrity and confidentiality; and (g) accountability.[505] The UK Data Protection Act, 2018 provides for six excluding accountability.

Lawfulness, Fairness and Transparency Principle

This principle has its root in the openness principle under the OECD Guidelines. It stipulates that personal data must be processed in a lawful, fair and transparent manner.[506] In order words, personal data can only be processed where there exists one or more legal or lawful bases, reasons, factors or events permitted by the law of respective country where the data subject is resident or controller does business.[507]

Under this principle, the collection, use, management, destination, transmission, and all other activities performed on personal data must be done according to the dictates of prevailing law or in a manner that does not contravene any extent law at the time of such activity. The principle has three limbs: (a) lawfulness (b) fairness and (c) transparency.

Lawfulness

When processing personal data, handlers (controllers, processors, third parties, or recipients) must ensure that such dealings with personal data do not breach any applicable law(s) and they must

505 GDPR, art. 5.
506 NDPR, reg. 2.2.
507 Paul Voigt, EU General Data Protection Regulation GDPR: A Practical Guide (Springer International Publishing, 2017) 87.

prior to such processing identify the lawful/legal bases upon which they are dealing with the data in the first place.[508] Processing will be deemed unlawful where it contravenes a privacy or data protection law, infringes intellectual property law, constitutes a breach of law(s) regulating contractual relationships, breaches sector–specific regulation, rules or practices or violates any other law of the land.[509] Processing is however lawful if processed pursuant to any one or more legal bases to wit: (i) processed with data subject's consent (ii) for the performance of a contract to which the data subject is a party or about to enter (iii) for the compliance with a legal obligation (iv) in public interest (v) for data subject or third party's vital interest (vi) for legitimate of controller or third party.[510]

Fairness

The history of this principle is traceable to 1973 and the resolutions of the Council of Europe which made reference to 'fair collection of data and unfair discrimination.[511] Fairness as a principle of data protection has been noted to lack a precise definition,[512] it is unlike lawfulness, vague but for processing to be fair, data subjects must be fully aware of processing activities and the entire circumstances surrounding same. [513] Sandru describes 'fairness' as the 'heart' of data protection principles and that its pre–eminence is particularly pronounced by its ubiquity in all

508 Nicola Fabiano, 'Ethics and the Protection of Personal Data' (2019) IMCIC 2019–10th International Multi–Conference on Complexity, Informatics and Cybernetics, Orlando, Florida, USA, 1–17.
509 Lydia F. de la Tore, 'What Does Lawfulness, Fairness and Transparency Mean under EU Data Protection Law' (2019) < https://medium.com/golden–data/what–does–lawfulness–fairness–and–transparency–mean–under–eu–dp–law–a385d249d754 > accessed 11 May 2021.
510 These are considered in detail later.
511 Resolutions (73)22 and 74(29) were adopted to set up systems prohibiting unfair collection and processing of data Council of Europe Convention 108 and Protocols found at < https://www.coe.int/en/web/data–protection/convention108/background> accessed 11 May 2021.
512 Damian Clifford, 'Fairness and the General Data Protection Regulation–Operationalising Fairness in Data Protection Impact Assessments' Report Commissioned by Office of Data Protection officer at Facebook < https://hmi.anu.edu.au/ourwork/fairness–and–the–general–data–protection–regulation> accessed 19 June 2021.
513 Zuiderveen Borgesius 'Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis, University of Amsterdam, 2014).

data protection laws.[514] The principle has also been described as 'the most fundamental criterion' and 'core principle' of lawful processing of personal data.[515]

The principle requires controllers to balance the interests and legitimate expectations of data subjects by ensuring that such processing activities do not negatively impact vulnerable data subjects.[516] Data controllers are fair to data subjects when they are able to legitimately gain data subjects' trust in their processing activities. Conversely, processing activities are fair where data controllers are able to legitimately gain data subject's trust in the entire process by ensuring the latter clearly understands what personal data is required or collected, the purpose of collection and the likely associated risks.[517]

In the legislative build up to England's first data protection law in 1978, the Lindop Report elaborated on the fairness principle thus:

> *"...the means by which balances are struck and the conditions under which the agreements between data subjects and data users are reached are of great importance. Where the agreements are voluntary the result will not be fair unless each party fully understands the requirement of the other, and there is a clear understanding of what data over to be provided and for what purposes they will be used. Fairness requires openness in such dealings, and it also requires that no advantage*

514 Daniel–Mihail Sandru, 'The Fairness Principle in Personal Data Processing' (2019) 10(2) Law Review 60,61.
515 European Data Protection Supervisor, 'Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data (EDPS) (2016) Opinion 8/2016 8 < https://edps.europa.eu/sites/default/files/publication/16–09–23_bigdata_opinion_en.pdf> accessed 10 May 2021.
516 Lee A. Bygrave, Data Protection Law: Approaching its Rationale, Logic and Limits (Kluwer International, New York, 2002.) 110.
517 European Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European Data Protection Law* (Publication's Office of the European Union, 2014).

should be fallen of any disparities in bargaining power.'[518]

According to Bygrave, the principle of fairness connotes that, in every processing activity, data controllers must consider the interest and reasonable expectations of data subjects, they must not underplay the stakes of subjects while pursuing their businesses or other data processing targets.[519] To achieve fairness in processing data, controllers must strike a fair balance between their own interest and data subjects' rights and must not process personal data in a way that disproportionately infringes fundamental rights and freedom of data subjects.[520] The determinant of fairness is data subject's actual knowledge of processing activities concerning him and the detailed ramifications of such processing. Malgieri argues that other means of fairness are non–discrimination, fair balancing, procedural fairness, bonafide dealings with data etc.[521]

In *Google Spain's* case, a man complained that Google's continued storage of his personal data relating to his social security debts (which he considered outdated and irrelevant) on Google's search engine was unfair to him, among other claims. When the case got to the CJEU, the court observed that, a fair balance ought to be struck between Google's interest and the man's fundamental right, hence Google ought to remove the data subject's sensitive information from the web pages as it was unfair on him. The court specifically held that: "the balancing to be carried out ……. enables account to be taken …. of all the circumstances surrounding the data subject's particular situation.'[522]

518 Norman Lindop, Report of the Committee on Data Protection, (Her Majesty's Stationary Office, 1987) 11.
519 Ibid.
520 Damian Clifford and Jeff Ausloos 'Data Protection and Rule of Fairness' (2018) 37(1) Yearbook of European Law, 130–187.
521 See Gianclaudio Malgieri, 'The Concept of Fairness in the GDPR' A Linguistic and Contextual Interpretation' (2020) Proceedings of the 2020 Conference in Fairness, Accountability and Transparency, 154–166.
522 See Google Spain SL, Google Inc. v AEPD. Case C–131/12; Casebook on Data Protection (Noetico Repertum, Lagos, 2020) 490.

Transparency

Although, it had always been a key concept of European law, transparency was never a principle of data protection, at least in Europe, until it was introduced into the GDPR in 2016.[523] It was not contemplated by the Data Protection Directive 95/46/EC as a principle even though member states were duly bound to 'ensure' transparency of processing in their territories[524] but at the 31st edition of International Conference of Data Protection and Privacy Commissioners held in Madrid, Spain in November 2009, discussions were held on the essentiality of inclusion of transparency of processing activities in the GDPR.[525]

Transparency has been comprehensively described as 'an act of almost perfect communion between those who decide to process data (the data controllers) and the individuals linked to such data (the data subjects) during which the latter get to actually see and properly understand what is going on with their data, why this is occurring at all, what will happen to them and their data in the near future and what they could do about it, in case they would like to do something about it.'[526]

The objective of transparency as a principle is the provision of information to people what kind of information about them are collected or dealt with by whom, the circumstances of such dealings and any consequences or implications of same. It

523 Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/6 79) < https://ec.europa.eu/newsroom/article29/items/622227> accessed 12 May 2021.

524 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,** recital 63.

525 Heike Felzmann, Edward Fosch Villaronga, Christoph Lutz and Aurelia Tamo–Larrieux 'Transparency You Can Trust: Transparency Requirement for Artificial Intelligence Between Legal Norms and Contextual concerns' (2019) Big Data & Society 1, 2.

526 Gloria Gonzalez Fuster, 'Transparency as Translation in Data Protection' in Emre Bayamilogu, Irina Baraliuc, Liisa Albertha Wilhelmina Janssens and Mireille Hildebrandt, (eds) *Being Profiled: Logitas Ergo Sum: 10 Years of Profiling the European Citizen* (Amsterdam University Press, Amsterdam, 2018).

requires that controllers must not only inform data subjects on the collection, use, consultation, transmission, and other activities on their personal information, they must also ensure that all processing activities on such personal data are easily accessible and communicated in a simple manner to the data subjects, i.e processing must be as open and transparent as possible.

Transparency in this context could be prospective or retrospective: it is prospective when a data subject is informed about impending processing activities on his personal data before such activities occur at all[527] and retrospective when controllers disclose to data subjects processing that had been done on their personal information after the fact–this is also referred to as the 'right to explanation.'[528] In showing transparency, controllers must effectively give data subjects information on their identities kept by the controller, purpose of processing, data subject's rights and how to exercise them, the risks associated with processing and safeguards, possibility of sharing with third parties, etc[529] with layered privacy notices are advisable for data controllers to ensure high level transparency of the business operations. This specie of notices was devised to provide data subjects with high level but simplified and summarized privacy information with the option of reading more detailed privacy notice on another page.[530]

The NDPR does not however list transparency under the principles but as a right of data subjects by requiring data controllers to

527 Bryan Casey, Ashkon Farhangi and Roland Vogl 'Rethinking Explainable Machines: The GDPR's Right to Explanation' Debate and the Rise of Algorithm Audits in Enterprise' (2019) 34(1) Berkeley Technology Law Journal, 143–188.

528 Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7(4) *International Data Privacy Law*, 233–242; Sandra Wachter, et al 'Why a Right to Explanation of Automated Decision Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law*, 76.

529 Paul Voigt, *EU General Data Protection Regulation GDPR: A Practical* Guide (Springer International Publishing, 2017) 87.

530 Patrick Gage Kekey, Lucian Cesca, Joanne Biesse & Loririe Faith Crenor, 'Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach' (2009) The Proceedings of the 28th International Conference on Human Factors in Computing Systems, CHI 2010, Atlanta Georgia, USA, April 10–15, 2010.

provide data subjects with information relating to processing activities on their personal data in a transparent manner.[531] The transparency principle ultimately imposes three obligations on a data controller: (i) provision of information to data subjects on processing activities with or without request; (ii) communication of data subjects' rights in an intelligible and simple manner and (iii) facilitation of the exercise of rights communicated to the data subjects.

Purpose limitation principle

This is one of the fundamental principles of data protection law, the origin of which is traceable to the earliest conversations around the concept of data protection.[532] The principle effectively assigns controllers the duty of ensuring that personal data is only processed for the original purpose of access or collection[533] by mandating controllers to ensure that personal data are not used for incompatible purposes.

In complying with this principle, controllers must be clear from the outset on what purpose the personal data demanded or processed was meant for and they must not use such information for other incompatible purpose(s) i.e. the reasons for collection must be unequivocal and they must not deviate from same.[534] Controllers are duty–bound to disclose to data subjects transparently and proactively, at the earliest stage of processing, the purpose for collection of data and they must not process such data in an incompatible manner with the initial purpose disclosed. This

531 NDPR, reg. 3.1(1).
532 Maxmilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws* (Nomos Verlagsgeselischaft mbH, Baden–Baden, 2018) 31.
533 NDPR, reg. 2.1(a).
534 A common example of violation of this principle is found in cases where telephone subscribers' numbers are shared with other organisations for direct marketing purposes. See the Court of Appeal's decisions in Emerging Market Telecommunication Service v Eneye (2018) LPELR 46193(CA) and Godfrey Eneye v MTN Nigeria Communication (Unreported) CA/L/136/2009.

principle has two components: (i) purpose specification and (ii) compatible use which has been expanded in recent times.

Purpose specification

Purpose specification obligates data controllers to collect and strictly utilize data for 'specified, explicit and legitimate purpose' disclosed to the data subjects at the time of collection. This obligation compels controllers to preliminarily define the purpose of data before collection and in the context of collection, 'purpose' must be unambiguous, specific but not omnibus. Purpose statements like 'for commercial purposes', 'improving customer/user experience' or 'for advertising or communication purposes' are generally regarded as indefinite and imprecise purpose specification.[535] Purpose specification has three components: specified purpose, explicit purpose and legitimate purpose.

Specified purpose: This prohibits generalization of purpose i.e. the controller must be specific and definite in its disclosure of the particular purpose for which personal data is processed. The information supplied to data subjects must be sufficiently detailed and accurate enough to enable the former to make informed decision on whether to consent or not.

Explicit purpose: Here, the purpose must be simple, unambiguous and clearly explained to data subjects. This typifies the nexus between the principle of purpose limitation and transparency which underscores the data subject's expectations on the use of their personal data. However, where there is more than one purpose, the anticipated separate processing activities must be fully explained to the data subject.

535 Article 29 working Party, Opinion 03/2013 on Purpose Limitation (WP 203) 00569/13 EN, 16; see also Asia Biega and Michele Finck, 'Reviving Purpose Limitation and Data Minimization in Personalisation, Profiling and Decision–Making Systems' Max Planck Institute for Innovation and Competition Research Paper No. 21–24.

Legitimate purpose: Data controllers are obliged to use personal data only for purposes sanctioned by relevant and applicable laws. It is expected that personal data would not be utilized for purposes that comes in conflict with criminal law, employment law or even standard practices and customs.

Compatible use

In the event of further processing of personal data, again, such must not be incompatible with the original purpose. The compatibility test used here is however not cast in stone, as processing for another purpose does not necessarily render such incompatible provided it is sufficiently connected with the original purpose. To ascertain compatibility, the following factors have been advisedly devised for consideration: (a) existence of a nexus between original purpose and purpose for further processing; (b) context of the original collection and reasonable expectation of data subjects based on their relationship with the controller; (c) nature of personal data collected; (d) consequences of the further processing on data subjects; and (e) availability of sufficient safeguards.[536]

Data minimization principle

This principle stipulates that collection of data must be limited to the minimum amount of information expedient to achieve a certain purpose per time.[537] Data minimization is an offshoot of purpose limitation to the extent that, it also limits the quantum of data collected for a particular purpose and it is a cluster of

536 Wouter Seinen, Andre Walter and Sari van Grondelle, 'Compatibility is a Mechanism for Responsible Further Processing of Personal Data' https://www.bakermckenzie.com/–/media/files/insight/publications/2018/10/compatibility_mechanism_responsible_further_personal_data_processing.pdf?la=en > accessed 12 June 2021.
537 Meilof Veeningen, Benne de Weger and Nicola Zannone, 'Data Minimization in Communication Protocols: A Formal Analysis Framework and Application to Identity Management' (2014) 13 International Journal of Information Security, 529–569.

three requirements i.e., data collected must be: (a) adequate for purpose of collection; (b) relevant to purpose of collection; (c) limited to necessity of purpose.

Adequacy

This speaks to proportionality within the context of data collection.[538] Data controllers are required to collect personal data sufficiently adequate for the disclosed purpose and nothing more. This underpins the erstwhile principle of proportionality which necessitated suitability, non–excessiveness and necessity of data collected.[539]

Relevance

Here, only personal data that is patently relatable and valid for disclosed purpose can be collected and/or retained by data controllers who must be able to demonstrate the remote or direct nexus between data sought to be processed and the specific purpose disclosed for its processing. Relevance represents a check on controllers from indiscriminate accumulation of personal data without business or legitimate basis.

Necessity

Controllers are required to interrogate the granular forms of data sets necessary to achieve the organizational goal for such processing activities. In other words, controllers need to ascertain with exactitude the quantum of data required to achieve specific purposes, hence where a smaller amount of personal data can be utilized to achieve a certain objective, the utility of a larger set of

538 NDPR, reg. 2.1(b).
539 Fred H. Cate, 'The Failure of Fair Information Practice Principles' in Jane K. Winn (ed) *Consumer Protection in the Consumer Protection in the Age of Information Economy*, (Ashgate, Farnham, 2006) 341.

personal data would be adjudged unnecessary.[540] This obligation is not to absolutely meet data collection but one that requires data to minimize the sufficiency and adequacy level of the controller's need and specified purpose. The principal emphasis being the collection of the smallest quantum of data necessary to achieve the disclosed purpose.

Accuracy principle

Described as the 'bulwark' of data protection law,[541] the accuracy principle essentially stipulates that, controllers that use personal data in the ordinary course of their business operations must ensure that such personal data practically reflect the true status of the data subject.[542] While the principle has been taken for granted as the simplest of all data processing principles, personal data expressed in form of inferences and opinions formed from facts about data subjects, however, pose some difficulty when measured against the principle of accuracy which mandates such information to be reasonably correct.

The accuracy principle does not only regulate the collection of correct personal data, it also behoves controllers to keep such data up to date while accentuating the principle of data quality in the process.[543] This principle requires data controllers to take reasonable measures to ascertain accuracy of personal data and where expedient, keep such data updated. The term 'reasonable measures' could include verification of such information to ensure its completeness, accuracy and prevent it from misleading and

540 Asia J. Biega, Peter Potash, Hal Daume, Fernando Diaz, and Michele Fink, Operationalizing the Legal Principle of Data Minimization for Personalization' (2020) SIGIR, Virtual Event, China, 399, 400.
541 Dara Hallinan and Fredrick Zuiderveen Borgesius 'Opinions Can Be Incorrect. (In Our Opinion) On Data Protection Law's Accuracy Principle' (2020) 10(1) International Data Privacy Law, 1, 2.
542 NDPR, reg. 2.1(b).
543 Jiahong Chen 'The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle' (2018) 4 European Data Protection Law Review, 36, 37–81. Data quality in this context refers to the fitness of personal information for all purposes it is required for. See Shawn Turner, 'Defining and Measuring Traffic Data Quality' (2004) 1870(1) Journal of Transportation Research Record, 62–69.

where personal data is not collected directly from data subjects, controllers must necessarily verify the source of such information to confirm its credibility and currency.[544]

Storage limitation principle

This principle prohibits controllers from storing data for a longer period than it is necessary for the initial purpose of collection.[545] Hence, once data has outlived its purpose, it must be deleted or rendered anonymous or in some cases, pseudonymous. Anonymization is 'the process of turning data into a form that does not identify individuals' by erasing the nexus between personal data and data subjects and rendering direct or indirect identification impossible.[546]

In complying with this principle, controllers are meant to identify requisite retention periods for various kinds of personal data collected by them which period may be fixed by legislation, business practices or legitimate interest of controller or a third party. The principle prohibits indiscriminate and unjustifiable accumulation of personal data by controllers even after they have been put to their original use[547] and to fulfil this obligation, controllers are advised to set justifiable and realistic internal time limits for data retention in the absence of regulatory retention period.[548]

544 Eduardo Ustaran (ed), *European Data Protection Law and Practice* (IAPP, Brussels, 2019) 282.
545 NDPR, reg. 2.1(c).
546 Kristel Toom & Pamela F. Miller, 'Ethics and Integrity' Jan Andersen, Kristel Toom, Pamela F. Miller (eds) in *Research Management, Europe and Beyond*, (Academic Press, Cambridge, 2017) 263–287.
547 It discourages 'data graveyards'–storage of big data without use. See M. Bauer, 'Get Valuable Information From The Data Graveyard' (2007) < https://www.researchgate.net/publication/255579707_GET_VALUABLE_INFORMATION_FROM_THE_DATA_GRAVEYARD> accessed 30 June 2021.
548 Arianna Vedaschi and Valerio Lubello, "Data Retention and its Implications for the Fundamental Right to Privacy. A European Perspective' (2015) 20 Tilburg Law Review, 14–34.

Integrity and confidentiality principle

This twin principle stipulates that, to guarantee fair processing of personal data, such data must be secured from unauthorized use, alteration transmission, theft or corruption. Under this principle, while processing data, controllers are obliged to adopt technical and organizational measures that would secure data from unauthorized or unlawful handling of data especially by third parties. Most data protection legislation require data controllers to implement information security systems to preserve the integrity of personal data in their custody.[549]

Accountability principle

It is sometimes erroneously perceived that the accountability is a new principle, but it has been part of the conversations around European data protection law since the 80s when the principle surfaced in the OECD Guidelines and repeated in the 2013 updated version. [550]

This principle essentially obliges data controllers to take all appropriate measures to observe compliance with their obligations under applicable data protection laws and implement mechanisms to demonstrate such compliance.[551] The accountability principle was designed as a mechanism to build data subjects' trust in controllers' processing activities and serve as a tool to probe latter's fulfilment of their privacy promises as disclosed in their

549 NDPR, reg. 2.6.
550 Clause 14 provided that a data controller should be accountable for complying with measures which give effect to the principles stated above. See Organisation for Economic Corporation and Development (OECD), 'Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' 23 September 1980. < https://www.oecd.org/sti/ieconomy/2013–oecd–privacy–guidelines.pdf > accessed 12 June 2021.
551 NDPR, reg. 2.1(3).

privacy notices.[552]

It is worthy of note that, the accountability principle also extends to processing activities carried out by processors engaged by the controllers. The principle effectively checks abuse of (processing) powers by controllers who are in control of sensitive information about data subjects. The duty is two–pronged: controllers are accountable to data subjects on one hand and the supervisory authorities on the other[553] and to demonstrate fulfilment of this principle, controllers must periodically report compliance to supervisory authorities, clarify and justify their policies and business activities around their data processing operations. Essentially, businesses must internalize transparency to constantly demonstrate compliance through accountability–a process described as a form of 'enhanced responsibility'[554] which enforces a proactive demonstration of organizational capacity to observe contemporary data protection standards that in turn, engender data subjects and regulators' trust on one hand and as well as ensure mutually rewarding transparent business practices on the other.[555] The principle imposes a measure of responsibility on data controllers hence it has been described as 'principle of responsibility' in some legislation even though accountability is broader than responsibility.[556]

552 See Charles Raab, 'The Meaning of Accountability in the Information Privacy Context' in Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener & Hector Postigo (eds) *Managing Privacy Through Accountability* (Palgrave and Macmillan, London, 2012) 27.

553 Joseph Alhadeff, Brendan Van Alsenoy and J. Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions in Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener & Hector Postigo (eds) *Managing Privacy Through Accountability* (Palgrave and Macmillan, London, 2012) 42.

554 Colin J. Benett, 'The Accountability Approach to Privacy and Data Protection: Assumptions and Cavaets' in Managing Privacy Through Accountability, Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener & Hector Postigo (eds) (Palgrave and Macmillan, London, 2012) 27.

555 Lina Jasmontaite and Valerie Verdoodt 'Accountability in the EU Data Protection Reform: Balancing Citizens' and Business Rights' (2016) in Privacy and Identity Management. Time for a Revolution? Privacy and Identity 2015,476 IFCP Advances in Information and Communication Technology, 156–169.

556 Collin J. Bennet, 'International Privacy Standards: Can Accountability be Adequate? (2010) 106 Laws and Business International, 3.

CHAPTER TWELVE

Lawful bases for data processing

Under the principle of lawfulness, there are grounds for processing of personal data which the law regards as valid.[557] Where a controller is unable to rely on any of the bases to process data, then such processing activity is unlawful unless it falls under the provided exceptions[558] which exceptions vary per jurisdiction, but they are mostly identical. This chapter discusses each of the legal basis on after the other.

Where data subject has consented to processing activity

This ground or legal basis superficially appears to be the simplest of all, but experience has shown that it could also be the trickiest. It stipulates that personal data would be deemed to have been lawfully or legally processed where the data subject consents to such processing for one or more specific purposes. In this context, consent is understood as 'any freely given, specific, informed and unambiguous indication of data subject's wishes by which he or she, by a statement or by a clear affirmation action, signifies agreement to the processing of personal data relating to him or her.'[559] For consent to be valid, it must satisfy the following conditions:

557 They are interchangeably referred to as "lawful grounds," "legal grounds," "lawful bases" or "legal bases."
558 For example, processing for purely personal or household activities, criminal investigation, or prevention, historical, educational, research or journalistic or anonymised data. These are extensively discussed in a latter chapter.
559 GDPR, art. 4(11); NDPR, reg. 1.3(iii).

a. Must be freely given;
b. Must be specific
c. Must be informed
d. Unambiguous and
e. By an affirmative action

Freely given consent

When faced with a decision to give consent to the processing of their personal information, data subjects must be seen to have unhindered, uninhibited, and uninfluenced choice and control over such decision.[560] For example, where there is imbalance of (bargaining) power between data subject and controller, consent may not be freely given.[561] Schermer, et al describe this as the need to ensure 'absence of coercion by others' with the following instructive words:

"For consent to be valid, it must be freely given. Consent is not morally transformative, if it is not the result of an autonomous choice of the person giving the consent. Absence of control by others in the context of consent presupposed an element of choice: if refusing to consent is not a viable option, because it is either impossible or it would have a very negative impact on the person giving consent, then there is no real choice and thus no consent. As such, if a person is under duress or any form of undue influence the consent is vitiated.'[562]

Personal autonomy underpins the necessity for consent to be freely given. Consent is however freely given where a data subject

560 NDPR, reg. 2.3(2).
561 Orla Lynskey, *The Foundations of EU Data Protection Law* (1st edn. Oxford University Press, Oxford, 2005) 260; see also Benjamin Bergemann, 'The Consent Paradox: Accounting for the Prominent Role of Consent' in Data Protection (2018) in Marit Hansen, Igor Eleni Nai–Formo, Simone Fisher Habner (eds) *Privacy Identity Management. The Smart Revolution*, (Springer International Publishing, 2018) 111–131.
562 Bart W. Schermer, Bart Custers and Simon van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 11 Ethics Information Technology, 173.

is convinced to supply personal data provided there is no element of (subtle) threat.

Specificity

Consent must be directed at a specified request or action of the data controller. Hence, there must be sufficient clarity on the request which needs to be consented to, on one hand and clear indication of approval of such request by the data subject on the other hand. For consent to be valid, the data subject must have a clear understanding of the use of his personal information as well as where his consent is required. The processing activities and giving of consent must not give room for multiple interpretations, otherwise consent will be vitiated.[563]

In other words, any ambiguity in the data controller's actions and data subject's consent renders such consent invalid, hence, consent cannot be given for a blanket event, it must be directed at a specific action and ultimately, in data protection, consent cannot be implied, it must be expressed by an 'affirmative action.' There must be a nexus between the consent and the particular data processing operation contemplated and the controller at all material times must demonstrate conditions of the operation which requires consent and pro–actively communicate full details of same to the data subject.[564]

Informed consent

Informed consent guarantees that a data subject is pre–informed of the processing activities even before they take place. To appreciate

563 K.H. Satyanarayan Rao, 'Informed Consent: An Ethical Obligation or Legal Compulsion' (2008)1(1) Journal of Cutaneous Aesthetic Surgery, 33–35.
564 Christopher Kuner, Lee Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR). A Commentary* (Oxford University Press, Oxford, 2020) 183.

the nature of informed consent, full disclosure, voluntariness, competence to agree and a data subject's clear understanding of the implication of his/her agreement must be considered. [565]

Here, the data subject must not only be duly notified of the personal data collected and the risks associated with processing activities, but full disclosure must also be made of the identity of the controller, purpose of processing and the right to withdraw consent at any time. Hence, the mere execution of consent form by data subjects[566] does not exculpate data controllers of liability if the information provided is neither comprehensive nor explanatory enough to enable the former to make autonomous decision.[567]

Unambiguity

Here, consent must be expressed by 'a clear affirmative action' signifying the data subject's agreement to processing operation(s) on his/her personal information. Thus, where a data subject's indication of consent is unclear, then such would not pass the test of unambiguity. For consent to be unambiguous, it must eliminate all doubts as to the true intentions of the data subject and may be inferred under certain circumstances. Scholars and researchers are however torn between arguments on whether consent can be implied. While Strobl et al are of the view that the parameters for implying consent need to be clarified, especially within the context of special category of personal data,[568]Schermer et al however argue that consent would be inferred where the actions of a data

565 Batya Friedman, Edward Felten and Lynette I. Millett "Informed Consent Online: A Conceptual Model and Design Principles" < ftp.cs.washington.edu › 2000/12 › UW–CSE–00–12–02> accessed 28 May 2021.
566 In the decision in Suit No. FHC/IB/CS/90/2020 between Digital Rights Lawyers Initiative and National Youth Service Corps, the Federal High Court however erroneously refused to invalidate consent given by Corps members to the publication of their personal data in a public magazine on the eve of their passing our parade just because the Corps members signed consent forms.
567 Rashmi Ashish Kadam, 'Informed consent process: A Step Further Towards Making it Meaningful' (2017) 8(3) Perspect Clinical Research, 107–112.
568 Judith Strobl, Emma Cave and Tom Walley, 'Data Protection Legislative: Interpretation and Barriers to Research' (2000) 321(7265) BMJ, 890–892.

subject point in that direction and that the concept has subjective and objective components,[569] Kosta also illustrates that, consent may be inferred where a data subject drops his business card in a bowl at an event or where he has been informed of processing of personal data and does not object.[570]

Notwithstanding the academic intervention of scholars, the question can only be satisfactorily answered from the texts of the relevant laws, for example, in spite of the definition of consent which includes 'by statement' or 'clear affirmative action' in the English legislation[571] it has nevertheless been suggested to contemplate implied consent in certain circumstances, especially in online transactions.[572]

However, since in practice, consent does not only require an affirmative action on the part of the data subject but also a specific indication of the processing activities consented to, implied consent is not only impracticable, but it will also lead to a barrage of unauthorised processing and uninformed consent as we now witness on digital platforms and it must be noted that, the notion of inferred or implied consent may not also find support in the definition of consent which requires a 'clear and affirmative act' signifying agreement to processing operations.

In spite of the requirement for unambiguity, which is somewhat relaxed, some data protection legislation additionally require

569 Bart W. Schermer, Bart Custers and Simon van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 11 Ethics Information Technology, 173.
570 See Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, Leiden, 2013) 286.
571 Data Protection Act, 2018, section 84(2).
572 Information Commissioner's Office explains thus: "The idea of an affirmative act does still leave room for implied methods of consent in some circumstances, particularly in more informal offline situations. The key issue is that there must still be a positive action that makes it clear someone is agreeing to the use of their information for a specific and obvious purpose. However, this type of implied method of indicating consent would not extend beyond what was obvious and necessary." Found at < https://ico.org.uk/for–organisations/guide–to–data–protection/guide–to–the–general–data–protection–regulation–gdpr/consent/what–is–valid–consent/> accessed 29 June 2021.

'explicit consent' where sensitive data is processed. This specie of consent imposes more stringent conditions on data controllers to extract express statement of consent from data subject especially in writing. While unambiguity of consent protects personal autonomy, bodily integrity etc., explicit consent on the other hand focuses on the processing operation and imposes obligations on the controller to obtain demonstrated and more pronounced consent.[573]

Processing for performance of contract

A controller can lawfully process the personal data of a data subject with whom it intends to enter into contractual relationship or during the pendency of such contract.[574] This ground of lawful processing could play out in three ways: (a) where controller intends to contract with data subject, and it processes data in preparation for the content; (b) where controller processes data pursuant to its obligation under the contract or (c) where data is processed as a consequence or steps taken pursuant to data subject's request prior to contract. However, the question of what data is necessary to be processed for the entry into on performance of contract is one that must be considered in the light of the purpose and objective of such contract. It must however be noted that, reliance on the performance of obligations towards the entry or during the pendency of contract with a data subject or third party, as a legal basis, has an expansive coverage. It extends to all phases of contractual relationship: pre, during and post contractual stages, provided always that the controller can demonstrate the necessity of such processing for the contractual obligations contemplated thereunder. Processing will be deemed necessary if any obligation under the contract cannot be consummated or performed without

573 Mary Kirwan, et al 'What GDPR and Health Research Regulations (HRRs) Mean for Ireland: "Explicit Consent"–a Legal Analysis' (2020) 110 Irish Journal of Medical Science, 517.
574 NDPR, reg. 2.2(b).

such operation(s) and such processing is restricted to necessity for such contractual obligations.

For the performance of contract, consent cannot be relied on as an additional or sole ground, otherwise, it would be deemed involuntary and vitiated because performance of contract on its own is a ground for lawful processing, hence it ought not be muddled with consent which has its own nuances. Thus, where the performance of contract is dependent on consent, such consent cannot be deemed as necessary for such contract, hence it would not constitute a valid ground since performance of contract is a stand–alone ground for lawful data processing.[575] Conversely, consent will not be required as an additional ground where data is processed as a necessity for the entry or performance of a contract to which the data subject is a party. However, there may be some exceptional cases where consent would also be required for performance of contract, for example where personal data is volunteered as a collateral or consideration for performance of such contract.[576]

Processing in compliance with legal obligation to which the controller is subject.

Legal obligation is an obligation sanctioned by law and enforceable by court of law. It is the 'duty to do or not do something' 'a legal relationship in which one person, the obligor, is bound to render a performance in favour of another, the obligee.' [577]

Where a data controller processes data in fulfilment of a legal obligation, such processing operation is lawful but obligations

575 Paul Voigt, EU General Data Protection Regulation GDPR: A Practical Guide (Springer International Publishing, New York, 2017) 87.
576 Carmen Langhanke and Martin Schmidt–Kessel, 'Consumer Data as Consideration' (2015) 4(6) Journal of European Consumer and Market Law, 218–223.
577 Bryan A. Garner, *Black's Law Dictionary*, (11th edn, Thomson Reuters, 2019) 1929.

fixed by contract, custom or best practices will not necessarily pass as legal obligation within the context of this legal basis. [578] The legal obligation here may however be primary or secondary legislation [579] but there are instances where the law places an obligation on a private body to process data. For example, an employer is legally bound to process employees' data for tax, health insurance purposes etc. Hence, the applicable law must specifically stipulate the types of personal data to be processed, the recipient(s), the purpose of processing and in certain cases, the storage limit.[580]

Processing necessary to protect data subject's or another person's vital interest

Under this ground, a data controller may process personal data of data subject where such operation is in data subject's vital interest or that of another natural person.[581] The term 'vital interest' has been defined as an interest considered 'essential for the life of an individual.'[582]

Vital interests are essentially limited to matters of life and death especially for medical help when the data subject is unconscious or helpless and incapable of expressing consent or otherwise. It is instructive that this ground is not only fixated on the data subject but third parties as well i.e., where it is in a third party's virtual interest to process a data subject's personal data, this ground will avail such processing operation. For example, the personal information of a data subject may be processed where

578 NDPR, reg. 2.2 (c).
579 Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International Publishing, New York, 2017) 88.
580 Christos Giakoumopoulos, Giovanni Buttarelli and Michael O'Flaherty, *Handbook on European Data Protection Law,* (2018 edn, European Union Agency for Fundamental Rights and Council of Europe) 151.
581 NDPR, reg. 2.2(d).
582 It includes processing pursuing humanitarian objectives like prevention of spread of contagious diseases during emergencies etc. See Christopher Kuner, et al, *The EU General Data Protection Regulation (GDPR) A Commentary* (Oxford University Press, 2020) 333.

his neighbour, child or relative is involved in an accident and emergency medical procedure need to be observed but the victim could not immediately give consent. This legal basis is construed narrowly to accommodate only deserving circumstances[583] and resort is always had to this ground, where no other lawful ground for data processing exists and it interplays with public interest as well, even though matters of public interest are mostly determinable by law.[584]

Processing for task carried out in public interest, scientific or historical research

A data controller can lawfully process personal data where such operation is carried out as part of a task done in public interest.[585] In *Center for Oil Pollution Watch v National Petroleum Corporation,*[586] the Supreme Court defined 'public interest' as:

"...the general welfare of the public that warrants recognition and protection of something in which the public as a whole has a state especially, an interest that justifies government regulation.'

The objective of this ground is to provide a foundation for the collection and use of personal data in certain circumstances for the overall protection of the entire public or for research and journalistic purposes.

A private data controller cannot however rely on this ground without a legislation vesting it with the authority to carry out such task in public interest. For example, the English Act

583 Christopher F. Mondschein and Cosimo Monda, 'The EU's General Data Protection Regulation (GDPR) in a Research Context' in Pieter Kubben, Michel Dumontier, and Andre Dekker (eds) Fundamentals of Clinical Data Science, (Springer, International Publishing, New York, 2019) 62.
584 Emmanuel Ventrella, 'Privacy in Emergency Circumstances; Data Protection and the COVID–19 Pandemic' (2020) 21 ERA Forum, 379–393.
585 NDPR, reg. 2.2(e).
586 (2019) 5 NWLR (Pt. 1666) 516.

specifically provides that such authority must have been vested in the controller before personal data can be processed under this basis.[587] Processing activities that are usually contemplated are for the exercise of law–making function by a legislative body, discharge of function conferred by law, exercise of ministerial function, administration of justice etc.

Processing is necessary for the purpose of legitimate interest of data controller/third party

Just like vital interest, this ground permits a controller to process a data subject for its legitimate interest or that of a third party.[588] Legitimate interest in this context is also referred to as 'balance of interests' which presupposes that, a data controller can validly process data in the absence of other legal bases if the interest of the data subject does not prevail over the controllers. Hence, the ground conducts a balancing test between the rights and freedoms of a data subject with that of the data controller and/or third party and in certain circumstances, the interests of a controller or third party can override the rights and freedom of a data subject.[589]

The legitimate interest contemplated here could be a legal right, fundamental right, business or commercial in nature but they are not at large without parameters and must be within the confines of the applicable laws.[590] The legal basis allows a data controller or third party to validly process data when either of the entities can demonstrate existence of relevant and legally prescribed protection and safeguards for data subjects' personal data especially where the latter is effectively put in control of his/

587 Data Protection Act, 2018, section 8 emphasises 'in the exercise of the controller's official authority.'
588 This legal basis is not provided under the NDPR as a ground but as a right of data subject.
589 Irene Kamara and Paul De Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach' (2018) 4(12) Brussels Privacy Hub, 12.
590 Federico Ferreti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or The Winter of Rights' (2014) 51 Common Market Law Review, 846.

her data on one hand and the controller or third party is able to process such data to meet its business or organizational demands on the other.[591]

For legitimate interest to avail a controller or third party, they must prove that: (i) based on the parties' relationship, data subjects reasonably expect their data to be utilized for such purposes; (ii) the processing is not a legal obligation, but it accrues some benefit to the controller or data subject or both; there is little or no risk of interference with privacy. Legitimate interest could be relied on in the event of crime detection or prevention, information security, threat to public security or safety and in certain circumstances, direct marketing could also be done under the ground legitimate interest.[592]

591 For further reading on legitimate interest, see generally: Paolo Balboni, et al, 'Legitimate Interest of the Data Controller. New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection' (2013) 3(4) International Data Privacy Law, 245.

592 The UK Information Commissioner's office offered some guidance on this: '... you might be able to rely on legitimate interest for your direct marketing purposes if you can show the way you use people's data is proportionate, has a minimum privacy impact and is not a surprise to people or they are not likely to object to what you are doing. See Information Commissioner's Office, Direct Marketing. Code of Practice, (version 1.0) 34.

CHAPTER THIRTEEN

Derogation And Exemptions

As found in most (fundamental) rights, the enjoyment of right to privacy and/or data protection is not absolute, and they may be derogated upon or exempted in certain circumstances. In this chapter, I discuss the derogations and exemption of data protection laws under separate subheading.

Derogation of privacy/data protection

A derogation is the temporary suspension of certain rights recognized in human rights instruments or constitutional bill of rights. Whether data protection is viewed as right to privacy or a stand–alone right, it is limited in its application by other rights or considerations. By section 45 of the Constitution[593] privacy is derogated by any 'law' reasonably justifiable in a democratic setting made in the interest of (a) defence, public safety, public order, public morality or public health or (b) for the purpose of protecting the rights and freedoms of other persons. This provision has two important components worthy of consideration here: (a) any law; and (b) reasonably justifiable.

Any law: Surprisingly, this phrase has not attracted any reported appellate court decision perhaps this is because it superficially appears simple. However when the provision of the interpretation

593 Constitution of the Federal Republic of Nigeria, 1999 (as amended)

section of the Constitution is considered, some curiosity is aroused as to the import of the phrase. For the avoidance of doubt, section 318 of the 1999 Constitution defines 'law' as 'a law enacted by the House of Assembly.' In the same vein section, the Interpretation Act also defines 'law' as 'any law enacting or having effect as if enacted by the legislature of a state and includes any instrument having the force of law which is made under a law.'[594] From the foregoing unambiguous statutory provision, it appears crystal clear that derogation under section 45 of the Constitution can only be invoked in favour of States' laws as opposed to federal enactments.

Reasonably Justifiable: What is reasonably justifiable is not always easy to define or ascertain but dependent on the facts and circumstances of individual cases. The Supreme Court in *Olawoyin v Attorney General of Northern Nigeria*[595] laid some parameters for reasonable justification as: (i) necessity in the interest of public morality and (ii) moderation and proportionality to the subject matter. On the duty to prove reasonable justification of a law, Nwabueze argued that such burden rests on an applicant who claims unreasonableness of a law[596] while Ogbu argued otherwise that the State must establish that the law was reasonable in the first place.[597] On his own, Garba decries lack of statutory and judicial definition of reasonable justification but advocates that government must be required to justify the reasonableness of the laws as manifested in the word "justifiable" used in section 45 in a bid to balance the rights of the citizens and limitations imposed by law.[598] However, in a decision challenging some provisions of the Cybercrimes (Prohibition and Prevention etc.) Act 2015 as an

594 Interpretation Act, Laws of the Federation of Nigeria, 1990, Cap. 192, section 18.
595 (1962) 1 ANLR 324 at 327. Also, in Chike Obi v Director of Public Prosecution (1961)1 All NLR 186, the same court reiterated the court's duty to determine what is reasonably justifiable in a democratic setting.
596 Ben Nwabueze, *A Constitutional History of Nigeria*, (Longman, New York, 1982) 18.
597 Osita Ogbu, *Human Rights Law and Practice in Nigeria* (Snaap Press, Enugu, 2013) 233.
598 Ahmed Salisu Garba, 'Permissible Limitations to Freedom of Religion and Belief in Nigeria' (2020)15 Religion and Human Rights, 57–76.

interference with right to privacy, the Court of Appeal held that:

"Once an enactment or law is made by the legislature such as the Act under discussion, the presumption of regularity of official Act under section 168(1) of the Evidence Act, 2011 that it was made with the indication, belief and notion that it is reasonably justifiable in a democratic society under section 45(1) of the 1999 Constitution. The onus shift on the party ascertaining otherwise vide *Osawe v Registrar of Trade Unions*[599] where the Supreme Court held per the judgement prepared by Oputa JSC (now of blessed memory) that once the law is made, the onus is on the party challenging its constitutionality to show that it is not reasonably justifiable in a democratic society.'[600]

Notwithstanding the decisions of the courts which remain the position of our laws for the time being, derogation or limitation of human rights is a right or defence exercised by governments to interfere with human rights within the confines of relevant laws.[601] Hence, the State must be held duty bound to justify the reasonableness of such laws which it seeks to use as a defence for its violation or interference with human rights since in most cases, it is used as a shield where an applicant alleges interference with fundamental rights.

Exemptions

Universally, certain processing activities are exempted from the ambit of data protection laws and regulations. They are discussed hereunder:

599 (1985) 1 NWLR (Pt. 4) 755 at 770.
600 Incorporated Trustees of Paradigm Initiative & 2 Ors. v Attorney General of the Federation (2018) LPELR–46655 (CA).
601 Article 15 of the European Convention on Human Rights refers to it as 'right of derogation.'

Processing for purely personal or household use

Processing operations carried out jointly or solely for personal or household purposes do not always attract personal data protection as some actions are excluded from the ambit of legal implications or coverage when undertaken with no expectation or contemplation of business, professional or commercial activities or gains. The rationale for this exemption is hinged on the impossibility of the law to regulate exclusively private activities undertaken by individuals within the comfort of their homes.

The early draftsmen realized the need to circumvent unreasonable expectations of compliance with and enforcement of data protection obligations by individuals with respect to processing operations carried out in their respective private spaces hence, the exception.[602] It is worthy of note that this exemption simply absolves the controller of certain obligations under the data protection laws, but it does not rob a data subject of his rights where such processing interferes with or violates such rights and/or freedoms. Hence, while a controller who processes data in his private space and for personal purposes may not be expected to be transparent or implement technical and administrative security measures to protect data, a data subject on the other hand who is adversely affected by such household processing is not precluded from exercising his data subject's rights.[603]

For this exemption to apply, the processing activity must be a

602 Jiahong Chen, Lilian Edwards, Lachalan Urguhart and Derek McAuley, 'Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10(4) International Data Privacy Law, 279, 280.

603 See the decision in JQL v NTP (2020) EWHC 1349 (QB) where an applicant was awarded damages against her uncle for the unauthorised disclosure of her personal information within the family's closed Facebook group and Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta where the CJEU held that Jehovah Witness members house to house preaching does not qualify as personal or household processing. See Olumide Babalola, Casebook on Data Protection, (Noetico Repertum, Lagos, 2020) 288.

'personal' or 'private' one which is not in the public sphere.[604] On whether processing of activities in social media constitutes private or public activities, Xanthoulis argues that social networking sites (SNS) and user generated contents (UGC)[605] may create some problems in the determination of questions relating to status of individuals as data controllers in a bid to ascribe liabilities and he therefore concludes that, the extant laws need to provide further clarity on what constitutes private and public processing activities.[606]

Conclusively, the extent to which processing of data on social media is exempted from data protection obligations and liabilities is still unsettled.[607] However every case would be considered on its merit to apportion appropriate liabilities especially when rights and freedoms of data subjects are interfered with in the course of the purported purely personal and household processing activities.

Ultimately, what would pass as personal activities would always be viewed from the prism of those activities which are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others.[608]

Law enforcement/investigation activities

Statutorily, certain public bodies are empowered to investigate crime and generally enforce the law.[609] Hence, data protection

604 In Lindquist's case, a woman who published her colleagues' personal data on a publicly accessible website was precluded from relying on the exception. See Göta hovrätt v Bodil Lindqvist Case C–101/01, Olumide Babalola, Casebook on Data Protection, (Noetico Repertum, Lagos, 2020,) 7.
605 These are are also refered to as "user created contents.' They are contents like opinions, pictures, videos, posts etc, uploaded by social media users in the course of their use of the various digital platforms.
606 Napoleon E. Xanthoulis, 'Negotiating the EU Data Protection Reform: Reflection in the Household Exemption' (2014) Proceedings of the 5th Conference on E–Democracy–Security, Privacy and Trust in a Digital World, Springer CCIS series, vol. 441, 4.
607 Rebecca Wong, 'Social Networking: The Application of the Data Protection Framework Revisited' (2014) 2(2) Birkbeck Law Review, 317–348.
608 See the Advocate General's Opinion in Ryneš v. Úřad pro ochranu osobních údajů, (Case c–212/13) para 33.
609 Police, immigration authorities, tax agencies, courts and other judicial bodies etc.

obligations and inhibitions do not apply to law enforcement agencies when exercising such statutory functions.

Anonymized or anonymous data

Universally, data protection laws only apply to personal data but exempted from non–personal data. This presupposes two categories of personal data, the first is data that never relates to an identifiable individual and the other is the personal data that has been altered to remove every nexus to an identifiable individual. This category is referred to as 'anonymous data or anonymized data.'[610]Since anonymized data does not identify an individual, they are therefore exempted from the ambit of data protection laws.[611]

Data of deceased person or legal entities.

Fundamental rights are defined as 'inalienable human rights and basic moral guarantees that people in all countries and cultures allegedly have simply because they are people.'[612] However, while fundamental rights are predominantly enjoyed and enforced by living natural persons, there are situations when those rights can be enforced after the death of an individual. In *Nosiru Bello v Attorney General of the Federation,*[613] the Supreme Court allowed the enforcement of fundamental right to life of a deceased who was executed by Oyo State officials during the pendency of

610 Michele Finck and Frank Pallas, 'They Who Must Not Be Identified–Distinguishing Personal from Non–Personal Data Under the GDPR' (2020) 10(1) International Data Privacy Law, 11,13.
611 In Breyer v Germany (Case C-582/14), the CJEU noted that the principle of data protection does not apply to anonymous information, namely to personal data rendered anonymous in such manner. Some common techniques of anonymization are suppression, generalization aggregation, noise addition, substitution, etc. See Elizabeth Brasher 'Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation' (2018) 1 Columbia Business Law Review, 209–253.
612 El Rufai v Senate of the Federal Public of Nigeria (2014) LPELR–23115 (CA) and Salihu v Gana (2014) LPELR–23069 (CA), Ransome–Kuti v Attorney General of the Federation (1985) 2 NWLR (Pt. 6) 21.
613 (1986) 5 NWLR (Pt. 45) 828.

his appeal.[614] These decisions are however restricted to right to life which is in a class of its own and such decisions would not apply to enforcement of right to privacy which is dependent on the existence of a human being to function or be exercised.[615] However, since data protection is an offshoot of right to privacy, it is enjoyable by only living individuals for the protection of their personal autonomy among other things especially since the GDPR and English Act expressly exempt their application from deceased persons.[616] The NDPR is silent on this but since it references data privacy, which is traceable to section 37 of the 1999 Constitution, its protection only extends to living persons.

On legal entities

In Nigeria, while a legal person can also enjoy certain fundamental rights,[617] it is precluded from enforcing rights to personal liberty[618] or privacy except it enforces same on behalf of its members or subscribers.[619] Conversely, although the NDPR simply defines data subject as a 'person,'[620] it expressly states that the regulation only protects the data privacy of natural persons, hence the protection is restricted to natural persons.[621] It is worthy of note that, universally, data protection is predominantly offered to 'residents' which often contemplates natural persons, however countries like Switzerland, Norway, Luxemburg, Austria and

614 See also the decision in Dilly v Inspector General of Police (2016) LPELR–41452 (CA).
615 Amos Enabulele 'The Right to life or the Right to Compensation Upon Death: Perspectives on an Inclusive Understanding of the Constitutional Right to Life in Nigeria' (2014) 3(1) Afe Babalola University, Journal of Sustainable Development Law and Policy, 100, 111.
616 Recital 27 of GDPR provides that, 'the regulation does not apply to the personal data of deceased persons. Member states may provide for rules regarding the processing of personal data of deceased persons.' The English Data Protection Act, 2018, Chapter 12, section 3(3) also makes its provisions applicable to 'identifiable living individuals.'
617 See Onyekwuluje v Benue State Government (2005) 8 NWLR (Pt.928) 614, Kelvin Peterside v IMB (1993) 2 NWLR (Pt. 278) 710.
618 See First Bank of Nigeria v Attorney General of the Federation (2018) 7 NWLR (Pt.1617) 121.
619 The Fundamental Rights Enforcement Procedure Rules 2009 empowers associations or groups to bring fundamental rights enforcement actions on behalf of their members.
620 The Interpretation Act however defines a person to include legal persons, see section 18.
621 NDPR, reg. 1.1(a).

Italy offered data protection to legal persons with the justification that the extension provided a channel for the protection of such corporations or associations' members.[622]

622 Bart van der Sloot, 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two–Ticted System' System' (2015) 31 Computer & Security Review, 26, 40.

CHAPTER FOURTEEN

Processing of sensitive personal data

Protection of intimate or sensitive personal data[623] is the crux of data protection law. The definition of 'sensitive data' is capable of dejure and de facto delimitation[624] i.e., while successive data protection laws expressly list what constitutes sensitive data, the increasing effect of technology in human activities and habitual accumulation of data continues to widen the sensitive data net especially since sensitivity of personal data varies with their intimate nature and effect of their breach on the data subjects' privacy.

Managing sensitivity of personal information is one of the most striking features of personal autonomy and informational privacy, hence the nature of sensitivity always determines the level of security a data subject gives to protect access to such information.[625] It deserves maximum attention, security and legislative guidance on its handling and management and this perhaps, explains why many data protection legislation define sensitive personal data along the lines of their respective national

623 These are also referred to as 'special categories of data.' Art. 29 Data Protection Working Party, 'Advice Paper on Special Categories of Data (sensitive data)' (2011) < https://www.pdpjournals.com/docs/88417.pdf> accessed 29 June 2021.

624 Paul Quinn and Gianelaudio Malgieri, 'The Difficulty in Defining Sensitive Data' (2020) German Law Journal, 1.

625 Amitai Etzioni and Chirstopher J. Rice, *Privacy in a Cyber Age: Policy and Practice* (Palgrave Macmillan London, 2015) 73; Sabah Al–Fadaghi, 'How Sensitive is your Personal Information?' in Proceedings of the 2007 KCM Symposium on Applied Computing, New York Association for Computing Machinery, 165–169.

realities.[626]

The NDPR defines sensitive data as, 'data relating to religions or other beliefs, sexual orientation health, rue, ethnicity, political views, trade union membership criminal records or any other sensitive personal information.'[627] The phrase 'any other sensitive personal information' makes the definition expansive enough to accommodate financial data, income data,[628] marital information, social security numbers, e–mail passcode, genetic and biometric information etc.[629]

It is in consideration of its vulnerability that data protection laws require special kind of consent for the processing of sensitive personal data i.e informed and explicit consent must be sought and obtained by the controller from the data subject before such processing can be considered lawful.[630]

Processing of sensitive personal data is generally prohibited but there are permissible grounds for processing i.e. where explicit consent of the data subject is sought and obtained, where processing is done for the performance of legal obligation or exercise of data controller's right or in the field of employment, processing in the data subject or third party's vital interest, processing carried out for legitimate activities of controller with adequate safeguards, processing of data already manifestly made public, processing for judicial activities, processing for public interest processing for

626 Min Wang and Zuosu Jiang 'The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World' (2017) 11 International Journal of Communication, 3286–3305.
627 NDPR, reg. 1.3 (xxv).
628 Categorized as financial data in some jurisdiction but some researchers have advocated for the various data protection laws to be reviewed to include financial data in their definition of sensitive data. See Karen McCullagh, 'Data Sensitivity: Proposals for Resolving the Conundrum (2007) 2(4) Journal of International Commercial Law and Technology, 190–201.
629 Catherine Jasserand, 'Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data' (2016) 2(3) Eur. Data Protection Law Revision, 297.
630 Kart Pormeister, 'Informed Consent to Sensitive Personal Data for the Performance of Digital Consumer Contracts on the Example of 23 and Me' (2017) 6(1) Journal of European Consumer & Market Law, 17.

provision of health and medical facilities for archiving, scientific, historical and research purposes.[631]

Ultimately, data controllers have the additional duty to implement appropriate safeguards ensuring that the processing of sensitive data does not result in violation of data subjects' fundamental rights and freedoms.[632]

631 Christopher Kuner, et al, *The EU General Data Protection Regulation (GDPR) A Commentary* (Oxford University Press, Oxford, 2020) 377.
632 NDPR, reg. 2.6; see also Rossan Ducato, 'Data Protection, Scientific Research and the Role of Information' (2020) 37 Computer Law & Security Review, 1, 7.

CHAPTER FIFTEEN

Data Security

The term 'data security' is sometimes erroneously conflated with cyber security, rather, it refers to 'institutional rules and technical method that an institution uses to ensure that data is only accessed by authorized people.'[633] Data security is the choice of organizational practices and procedures that an entity adopts to safeguard unauthorized access or handling of personal data in the organisation's custody and this concept also extends to trustworthiness of personal data within the context of processing activities.[634]

The principle of integrity and confidentiality underpins data security[635] as it essentially obliges data controllers to implement appropriate technical and administrative measures to safeguard and secure personal data collected in the ordinary course of their business operations.[636] The mechanisms and technical measures for data security are inexhaustive, largely unregulated and are sometimes determined by organizational internal need and practices but I shall consider

633 Lauren Henry, 'Information Privacy and Data Security' (2015) Cardozo Law Review de Novo, 107, 111.
634 Elisa Bertino, 'Data Security: Challenges and Research Opportunities' (2013) Secure Data Management, 9–13.
635 The ICO refers to it as the 'security principle,' See Guide to General Data Protection Regulation (GDPR) (2021) <https://ico.org.uk/for–organisations/guide–to–data–protection/guide–to–the–general–data–protection–regulation–gdpr/security/#:~:text=A%20key%20principle%20of%20the,and%20physical%20and%20technical%20measures.> accessed 19 June 2021.
636 NDPR, reg. 2.6; see also P.T.J. Wolters, 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?' (2017) 7(3) International Data Privacy Law, 165.

Anonymization. This refers to the alteration or modification of personal data into a form that is incapable of identifying a data subject. It is a data security process aimed at destroying any link between personal data and the data subject such that it becomes practically impossible to identify the latter.[637] Anonymization of data is advisable in situations where sensitive data needs to be shared for statistics or research purposes. Since the users of anonymised data do not need the identities of the data subjects, hence de–identifying them protects and guarantees the latter's privacy and other fundamental rights.[638]

Pseudonymization

This process also involves alteration of personal data to an extent that it no longer identifies a data subject without additional identification information. This process, although falls short of the level of protection offered by anonymization, it also reduces the risk of unauthorized exposure of a data subjects' information when it is in a pseudonymized form.[639]

Other security measures

Most data protection laws do not particularly mandate particular data security measures to be implemented by data controllers, but professionals have suggested the following measures:

Encryption, to convert personal data into codes to forestall

637 Kristel Toom, Pamela F. Miller, 'Ethic & Integrity' in Jan Andersen, Kristel Toom & Pamela F. Miller (eds) *Research Management. Europe & Beyond* (Academic Press, Cambridge, 2017) 263–287.
638 Amin Aminifar, Yingve Lamo Violet Ka Pun and Fazle Rabbi, 'A Practical Methodology for Anonymization of Structural Health Data' (2019) SHI 2019. Proceedings of the 17th Scandinavian Conference on Health Informatic Informatics, Oslo, Norway, 1.
639 Miranda Mourby et al, 'Are Pseudonymized Data Always Personal Data? Implications of the GDPR for Administrative Research in the UK' (2018) 34 Computer Law & Security Review, 222–233.

unauthorized access.[640]

Access authorization is an organizational procedure or system that restricts general access to personal data but grant access to limited and specified persons. It helps organizations to manage and secure personal data in an auditable manner.[641]

Tokenization is similar but distinct from encryption. It is the process of modifying personal data into a string of characters known as 'token.' With tokenization, data controllers replace sensitive data with 'surrogate data' which has no value to third parties.[642]

640 The GDPR suggests this in recital 83; see also Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 JIPITEC, 163.) Cryptography is also sometime advised as a form of encryption. It is the science of using mathematics to encrypt and decrypt data and enables data controllers to retain sensitive data and share same without the risk of unauthorized access by third parties. See Omar Rayad, 'Cryptography and Data Security: An Introduction' (2018) < https://www.researchgate.net/publication/327388046_Cryptography_and_Data_Security_An_Introduction > accessed 15 June 2021.

641 Renata M. Carvalho et al, 'Protecting Citizens' Personal Data and Privacy Joint Effort from GDPR EU Cluster Research Projects' (2020) 217(1) SN Computer Science, 1, 13.

642 Z. C. Nxumalo, P. Tarwireyi, M.O. Adigun 'Towards Privacy with Tokenization as a Service' (2014) IEEE with International Conference on Adaptive Science & Technology (ICAST) 1–6. See also data masking, blurring, short codes, data obfuscation etc.

CHAPTER SIXTEEN

Rights of Data Subjects

THE MAIN OBJECTIVE of data protection law is to safeguard the rights and freedoms of data subjects, hence, just like consumer rights legislation, data subjects are provided with an array of rights enforceable against data controllers and in some cases against the regulators.[643] In this chapter, I consider the major rights of data subjects guaranteed by regular data protection laws.

i. Right to be informed (right to information)

Data subjects have the inherent right to be duly and timely notified by data controllers on the nature and quantum of their personal data in the latter's possession and the purpose of such processing operation(s).[644] This right places a demand on controllers' compliance with the transparency principle through full disclosure of their processing operations to the data subjects to enable the latter exercise sufficient control over his/her personal information.[645] The information must however be provided prior to the collection or at the time of collection of personal data with the details of: name of controller, types of data collected, retention period, sharing, data subject's rights, security mechanism, contact information of data protection officer (DPO) etc.[646]

643 NDPR, reg. 3.1.
644 NDPR, reg. 3.1.(1).
645 Gloria Gonzalez Fuster 'How Informed is the Average Data subject? A Quest for Benchmarks in EU Personal Data Protection' (2014) Revista de Internet Derecho y Politica 19, 92.
646 NDPR, reg. 3.7(7).

In providing information to data subjects, controllers are to use mechanisms that will supply the information in a simple, transparent, concise, intelligible, easily accessible and relatable form. Privacy statements are one of the major devices used by controllers to inform data subjects of the processing activities and purposes even though these statements may not always fulfil the simplicity and consciousness requirements.[647]

Privacy policies or notices are document drafted by controllers to provide data subjects with comprehensive information on an organization's personal data management including collection, use, storage, transmission, and overall handling of data.

The concept of privacy policy and privacy notice have however been erroneously used interchangeably in total disregard of their dissimilarities. While a privacy policy is an internal document of an organization which inform its employees of its privacy practices, a privacy notice is externally focused, informing customers, regulators and all others on the organization's data management practices. However, where information about the data subject is collected from other sources outside the former, the data controller is also duty bound to take pro–active measures to timely inform the data subject except such is impracticable.

ii. Right of access to data held by controller

This right, like right to be informed also finds expression under the fundamental principle of transparency.[648] This right guarantees data subjects' access to their personal data collected by data controllers and in exercising this right, data subjects can request

647 Rossana Ducato, 'Data Protection, Scientific Research and the Role of Information' (2020) 37 Computer Law and Security Review, 1, 8.
648 David Bainbridge and Graham Pearce, 'Tilting at Windmills–Has the New Data Protection Law Failed to Make a Significant Contributions to Right to Privacy' (2000) 2 Journal of Information, Law and Technology, 1.

from controller, a statement of their personal data processed by the former and such information must be provided free of charge (with exceptions)[649] in a concise, simple, and readable format.[650]

This is technically known as 'Data Subject's Access Request' (DSAR)–a request by a data subject in the exercise of his/her data protection right of access to data held by the data controller. It does not have to be in any particular form except the relevant law or the data controller has a prescribed form for making such requests.[651] The exercise of this right enables data subjects ensure compliance with data processing principles on the part of the controllers on one hand and it also helps data subjects determine whether to exercise their right to rectification on the other. The right effectively confers data subjects with latitude to: (a) confirm from the controller whether or not his/her data is processed; (b) obtain details of such personal data in controller's possession; (c) access to/copy of information must be provided in a readable and easily accessible format; and (d) request in any form or procedure provided by controllers.[652]

iii. Right to rectification of personal data

This right underpins the principle of data accuracy (quality) and data subject's control over their personal information in a controllers' custody.[653] It guarantees the data subject's confirmation that their personal information is processed by controllers in an updated version on one hand and also obliges controllers to ensure that personal data is accurate, up to date or deleted when

649 This request ought to be granted free of charge except it becomes repetitive and unreasonable.
650 Luca Bufalieri, Massimo La Morgia, Alessandro Mei & Julinda Stefa 'GDPR: When the Right to Access Personal Data Becomes a Threat' (2020) IEEE International Conference on Web Services (ICWS), 1.
651 Jes Auloos, Rene Mahieu & Michael Veale, 'Getting Data Subjects Rights Right. A Submission to the European Data Protection Board from International Data Rights Academics to Inform Regulatory Compliance' (2021) 10 JIPITEC, 1.
652 Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International Publishing, New York, 2017) 100.
653 NDPR, reg. 3.1(7)(h).

irrelevant or outdated. Where a data subject finds personal data kept by controllers inaccurate, he/she can exercise this right to have such error corrected.

Personal data in this context, may be in form of opinions, [654] comments or a controller's description of certain personal features of a data subject. For example, in the case of *Khelili v Switzerland*[655] where the applicant's occupation was inaccurately recorded as 'prostitute' she successfully challenged the inaccurate description. Also in *Peter Nowak v Data Protection Commissioner*, the CJEU noted that a data subject can apply for the rectification of examination score in certain circumstances.[656]

iv. Right to erasure or deletion

This is also known as the right to be forgotten, right to de–refencing, right to be de–indexed or right to suppression.[657] It is the data subject's right to demand that data controllers completely erase or delete their personal information from the latter's database.[658] The right is exercisable where: (a) personal data is no longer relevant to the purpose of collection; (b) consent is the basis of processing, and it has been withdrawn; (c) data subject objects to the continued processing of data; (d) controller processes data without legal basis etc. This right confirms data subject's entitlement to remove potentially destructive information about them from data controllers' platforms where such information interferes with their right to privacy, and it is deep–rooted in the privacy related notions of self–governance

654 See Dara Hallinan and Frederick Zuiderveen Borgesius, 'Opinions can be incorrect (In our Opinion) on Data Protection Law's Accuracy Principle' (2020) 10(1) International Data Privacy Law, 1.
655 See Olumide Babalola, *Casebook on Data Protection* (Noetico Repertum, Lagos, 2020) 230.
656 Ibid., 475.
657 Christopher Kuner 'The Court of Justice of the EU Judgement on Data Protection and Internet Search Engines' (2015) LSE Law Society and Economy Working Papers 3/2015.
658 NDPR, reg. 3.1(7)(h).

and self–determination.[659]

The right was reportedly created by the CJEU in its decision in *Google Spain's* case[660] where Mr. Gonzales requested Google to remove information concerning his social security debt on the ground that it had been fully resolved years earlier and the court noted that Google was obliged to remove such links containing information relating to the data subject.[661]

v. Right to restrict further processing of data

This right interplays with right to rectification and right to erasure. It is exercised where a data subject needs to make a decision on whether to request rectification or deletion of his information processed by the controller as well as in the event of a conflict between the parties. When this right is exercised, the data controller can only store data until the data subject decides further actions or steps to be taken except where the latter consents or the information needed to be processed for legal claims or protection of others' rights. The right is not absolute but exercisable in certain circumstances: (a) where data subjects doubt the accuracy of data processed by controller; (b) where processing has no legal basis but data subject does not want it deleted but prefers restriction until further notice; (c) where controller no longer requires the data but data subject may need them stored for certain legal claims; (d) where data subject has exercised his/her right to object to further processing of data pending rectification.

659 Andres Guadamuz, 'Developing a Right to be Forgotten' in Tatiana–Eleni Synodinou, Philippe Jougleux, Christiana Markou and Thalia Prastitou (eds) *EU Internet Law, Regulation and Enforcement* (Springer International Publishing, New York, 2017) 2.

660 Google Inc. Spain SL v Google Inc. Agencia Espinola de Protection de Dates (AEPD) and Mario Costeja Gonzales. ECLI:EU:C: 2014:317.

661 Yann, Pandova, 'Is the Right to be Forgotten a Universal, Regional or 'Global' Right?' (2019) 9(10) International Data Privacy Law, 15.

vi. Right to data portability

This is a data subject's right to obtain his/her data and to transfer it to another controller or substitute data stored on a compatible platform[662] and in the exercise of this right, a data subject can re–utilize his/her personal data on multiple interoperable platforms.[663] The right interplays with competition law and consumer rights where data subjects can apply to their service–providers for the transfer of their existing data with them to another service–provider but the right is particularly exercisable: (a) where processing is done by automated means; (b) processing was indirectly carried out by data subject's consent; (c) processing is required for performance of contractual obligations.[664]

In exercising the right, data subjects are entitled to receive their personal data provided to the controller in a structured, commonly used, and machine–readable format' and to transfer same to another controller of their choice provided always that the controller reasonably has the capacity to effect such transfer.[665] The right was introduced into Europe by the repealed Data Protection Directive 95/46/EC as a novel additional right of data subject[666] and it effectively enforces free access to data, open formats, independence and choice of platforms and free erasure of data.[667] The format of transfer is an important feature of this right,

662 NDPR, reg. 3.1(15).
663 Helena Ursic, 'Unfolding the New–born Right to Data Portability: Four Gateways to Data Subject Control' (2018) 15(1) Journal of Law, Technology & Society, 42–69.
664 Chris Jay Hoofnagle, Bart van der Sloot, Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What it is and What it Means? (2019) 28(1) Information & Communications Technology Law, 65–98; Sarah Turner et al, 'The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IOT) Environment' (2020) New Media of Security, 1–21.
665 Janis Wong and Tristan Henderson 'The Right to Data Portability in Practice: Explaining the Implications of the Technology Neutral GDPR' (2019) 9(3) International Data Privacy Law, 173, 174; Maurizio Borghi, 'Data Portability and Regulation of Digital Markets' (2019) Centre for Intellectual Property Policy & Management, Working Papers No. 02–2019, 3.
666 Bart Custers & Helena Ursic, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6(1) International Data Privacy Law, 4–15.
667 Maurizi Borghi, 'Data Portability and Regulation of Digital Markets' (2019) Centre for Intellectual Property Policy & Management, Working Papers No. 02–2019, 3.

hence, it must be electronic, well structured, machine–readable and a commonly used version.[668]

vii. Right to object to processing

Unlike right to restriction of further processing, this is a complete right which further underpins data subjects' control over their personal data and it may be exercised in two instances: one, outright objection to entire processing activities and secondly, objection to direct marketing. In exercising this right, the data subject may request a controller to immediately suspend and halt all processing activities on his/her personal data even where same were initially collected with the data subject's consent on one hand and the right presupposes data subjects' entitlement to object to marketing activities of the controllers on the other hand.[669]

viii. Right not to be subjected to automated decision making

An individual who is subjected to an automated decision–making process which affects his rights, opportunities and/or entitlements is entitled to full and meaningful explanation of the decision–making process. The explanation of the process must be simple, clear and explicit enough for the comprehension of a layman.[670] Although this right outrightly prohibits the subjection of data subjects to automated decision–making process, it however gives some latitude in the event that such process becomes inevitable where data subject gives explicit consent, or it is necessary for the entry or performance of contract. Automated profiling is often part of automated decision making where data subject's personal data are used to assess his personal attributes or features in

668 Paul de Hert et al, 'The Right to Data Portability in the GDPR: Towards User Centre Interoperability of Digital Services' (2018) Computer Law & Security Review, 193–293.
669 Ibid.
670 Andrew Selbst and Julia Poules 'Meaningful Information and the Right to Explanation' (2017) 7(4) International Data Privacy Law, 233–242.

relation to his standards/characteristics of living for the purpose of predicting his preferences of his economic, social, health, religious, political choices and general personal interests and concerns.[671] While transparency principle requires data controllers to disclose information on automated decision–making in their business operations, the accountability principle mandates them to meaningfully explain and demonstrate that the algorithm[672] used for such decision–making are accurate, meaningful and not discriminatory.[673]

ix. Right to lodge complaint with supervisory authority

This right was introduced in Europe pursuant to the European fundamental right to an effective remedy.[674] Without prejudice to data subjects' right to ventilate issues concerning violation of their rights in court under the relevant data protection laws, they have the right to simultaneously lodge complaint with the supervisory authority against an erring data controller except where the relevant law makes such complaint a condition precedent to litigation. Upon lodgement of complaint, the supervisory authority is duty bound to investigate and resolve the issues within the time frame provided by relevant laws and impose the applicable fine or award appropriate damages where it is so empowered.

Article 4.2(1) guarantees a data subject's right to seek redress

671 Profiling is also the aggregation of personal data for the purpose of practicing unknown features or future behaviour of the data subject. See Frederike Kaltheuner and Elettra Bietti 'Data is Power: Towards Additional Guidance on Profiling and Automated Decision–Making in the GDPR' (2018) 2(2) Journal of Information Rights Policy and Practice, 1.

672 Algorithms in this context, are rules or process for calculations or other problem–solving procedure for computers. They are a sequence of instructions to complete a computer related task.

673 Lokke Moerel and Maijin Storm, 'Automated Decision Based on Profiling. 'Information, Explanation or Justification' that is the Question' in Nikita Aggarwal, Horst Eidenmuller, Lucas Enriques, Jennifer Pyne, Kristin van Zwieten (eds) *Autonomous Decisions and the Law* (C.H Beck–Hart–Nomos, Londong,2019) 1.

674 See article 13 of European Convention on Human Rights and article 47 of the Charter of Fundamental Right of the European Union. See also Wojciech Piatek, 'The Right to an Effective Remedy in European Law: Significance, Content and Interaction' (2019) 6 China–EU Journal, 163–174.

from the DPA without prejudice to his right to seek redress in court but in the case of *DRLI v Unity Bank,*[675] the Federal High Court however interpreted the provision to constitute a condition precedent to judicial remedy. The court held that the right to lodge complaint to the supervisory authority must be exercised before a data subject can approach the court.[676]

With respect, the position of the court is erroneous when the import of the phrase 'without prejudice' as used in regulation 4.2(1) NDPR is considered. The Court of Appeal defined the phrase 'without prejudice' as 'without loss of any rights in a way that does not harm or cancel the legal rights or privileges of a party'[677] hence, the provision should not have been interpreted as constituting a condition precedent that must be fulfilled before a data subject can approach the court seeking remedies for data breach.

675 Suit No. FHC/AB/CS/85/2020 (Abeokuta division).
676 Per Ibrahim Watila, J. (of blessed memory).
677 Federal Ministry of Health v The Trade Union Members of the Joint Health Sector Unions (2014) LPELR–23546(CA).

CHAPTER SEVENTEEN

Data Protection Authority

The regulator of data protection is universally and generically referred to as the 'Data Protection Authority' (DPA) or 'Supervisory Authority' (SA) which terms have been used preferentially or interchangeable in some legislations.[678] DPA is 'a relevant public body (i.e an independent regulatory agency, 'competent authority') empowered to perform supervisory functions in the field of privacy and data protection; these usually include monitoring, advising, investigating, intervening, suing, and hearing claims.'[679]

DPAs generally supervise and ensure compliance with data protection laws through investigation, resolution of disputes and imposition of sanctions where necessary.

In Nigeria, there is no statutorily assigned DPA but the NDPR contemplates a number of DPAs with different regulatory roles[680] but under this chapter, NITDA is focused as the main DPA in Nigeria while analysing its establishment, functions and role–playing under the NDPR.

678 The GDPR provides for 'supervisory authority' while the ECOWAS Supplementary Act recognises 'data protection authority.'

679 Dariusz Kloza and Anna Moscibroda, 'Making the Case for Enhanced Enforcement Cooperation Between Data Protection Authorities: Insights from Competition Law' (2014) 4(2) International Data Privacy Law, 120, 121.

680 The NDPR in one breath defines 'relevant authorities' to mean 'NITDA or other public bodies regulating personal data' (reg. 1.3(xxiv), it also defines 'the agency' to mean NITDA, (see reg. 1.3(xxvi) but in another provision, renders data controllers and processors accountable to 'regulatory authorities' (see reg 2.4(b) and then in another provision, references a 'supervisory authority' (see reg. 31.2) but ultimately confers right to lodge complaint for rights violations with a 'relevant authority' (see reg. 3.1(7)(j).

In March 2001, the federal government announced its National Information Technology Policy which execution cumulated in the creation of NITDA as the implementation agency. The agency started out on the 1st day of April 2001 as an office under the Federal Ministry of Science and Technology (the ministry) to provide information communications technology (ICT) tools to some secondary and tertiary institutions in Nigeria.[681] The agency was established to predominantly implement the IT Policy, regulate monitor, evaluate and verify progress under the supervision of the ministry.[682] However, in 2007, NITDA's creation as a public body was formalized by the enactment of NITDA Act (enabling Act) which established the agency as a body corporate with perpetual succession and juristic personality.[683]

Unlike other data protection laws which create their DPAs[684], NITDA conversely issued its own data protection regulation in spite of ranging arguments on its legitimacy to regulate data protection under section 6(a) and (c) of its enabling Act[685] which provision only empowers NITDA to regulate 'electronic data interchange' as opposed to regulating and imposing fines for personal data breach.[686] Jemilohun and Akomolede also argued

681 Patience I. Akpan–bong, *Information and Communication Technologies in Nigeria: Prospects and Challenges for Development* (Peter Lang Publishing, Bern, 2009) 203.

682 Tega Rexwhite Enakhire, 'The Nigerian National Information Technology (IT) Policy' in Eshareniana E. Adomi (ed.) *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements in Information Science Reference* (New York, 2011); G. Ajayi, 'African Response to the Information Communication Technology Revolution: Case Study of the ICT Development in Nigeria' African Technology Policies Study (ATPS) Special Paper 8, African Technology Policy Network, Nairobi, Kenya.

683 National Information Technology Development Agency Act, Laws of the Federation 2007, published in the Federal Republic of Nigeria Gazette No. 99 Vol.94 on the 5th day of October 2007, section 1(1) and (2). See also Lukman Ibraheem Diso, 'Information Technology Policy Formulation in Nigeria: Answers without Questions' (2013) 37(4) The International Information and Library Review, 295–302.

684 It is however worthy of note that some other DPAs in Africa were not actually created by the relevant data protection laws but by other enabling legislation. For example, the Angolan Law 22/11 of 2011 regulates data protection and Decree 214/16 of October 2016 created the DPA.

685 Section 6 (c) empowers NITDA to: 'Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper–based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information.'

686 Emmanuel Salami, The Nigerian Data Protection Regulation: Overview, Effects and Limits' (2019) < https://www.datenschutz–notizen.de/the–nigerian–data–protection–regulation–2019–overview–effects–and–limits–3522349/> accessed 10 April 2021.

that, there exists no nexus between the agency's statutory powers and data protection.[687] Notwithstanding the adverse arguments on the propriety of its issuance of the NDPR, NITDA has regulatorily assumed the position of Nigeria's DPA and such role–playing is yet to be judicially challenged or debunked.

Functions and powers under NITDA Act

Since NITDA is a creation of statute, its powers, functions, and duties are necessarily dictated by its enabling Act. However, for the purpose of this chapter, only the relevant portion of section 6 NITDA Act shall be considered. The section empowers NITDA to: "Develop guidelines for electronic governance and monitor use of electronic data interchange and other forms of electronic communication transaction as an alternative to paper–based methods in government, commerce, education, the private and public sectors, labour and other fields where the use of electronic communication may improve the exchange of data and information."[688]

a. Development of guidelines for electronic governance (e–governance)

NITDA Act does not define the term 'electronic governance' but it defines 'electronic record' as 'data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer–generated microfiche.[689] Conversely, a number of researchers have however defined the term 'e–governance' from divergent perspectives but with a common denominator. Ojo views it as an accepted methodology involving the use of information

687 Bernard Jemilohun and Ifedayo Akomolede, 'Regulations or Legislation for Data Protection in Nigeria? A Call for a Clear Legislative Framework' (2015) 3(4) Global Journal of Politics and Law Research, 1–16.
688 NITDA Act, s. 6(c).
689 NITDA Act, s.34.

technology in improving transparency, providing information speedily to all citizens, improving administration efficiency and improving services such as transportation, power, health, water, security, and municipal services.[690] E–governance has also been defined as 'public sector's use of information and communication technology in order to improve the delivery of information and service, thereby encouraging citizens' participation in the decision–making process.'[691] The term is often used interchangeably with 'e–government' which surfaced with digital transformation of governance almost over two decades ago[692] but such conflation downplays the asymmetries of both concepts.[693]

The concept has been variously defined as: 'a technology mediated service that facilitates a transformation in the relationship between government and citizens'[694] 'the commitment to utilize appropriate technology for a variety of ends including greater democracy and fain and efficient services'[695] 'internally focused use of ICT to manage organizational resources and administer policies and procedures'[696] 'the use of ICT to improve the quality of services and governance'[697] and ''the whole spectrum of the relationship and networks within government and networks regarding the usage

690 John Sunday Ojo, 'E–Governance: An Imperative for Grassroot Development in Nigeria' (2014) 6(4) Journal of Public Administration and Policy Research, 78.
691 Upmith Singh, 'E–Governance Implementation–A Literature Review Analysis' (2019) 6(1) International Journal of Research and Analytical Reviews, 459.
692 Frank Bannister and Regina Connolly, 'Defining E–Governance' (2012) 8(2) E–Service Journal, 3–25.
693 Donald J. Calista and James Melitski, ''E–Government And E–Governance: Converging Constructs of Public Sector Information and Communications Technologies' (2007) 31(1) Public Administration Quarterly, 87–120; Dibie et al prefer the term 'e–government' to e–governance and defined the former as the efforts of government to use interact to simplify its activities for both the citizens and public administrators. See Robert A. Dibie, Maryam Quadri, 'Analysis of Effectiveness of E–Government in Federal Government of Nigeria, (2018) 8(3) Journal of Public Administration and Governance, 76.
694 Kate Oakley, 'What is E–Governance' (2010) Integrated Project 1. e–Governance Workshop, Strasbourg, 10–11.
695 Thomas B. Riley, Electronic Governance in Context, Electronic Governance and Electronic Democracy: Living and Working in Connected World (Commonwealth Secretariat, 2000).
696 Shailendria Palvia and Sushil Sharma, 'E–Government and E–Governance: Definitions/Domain Framework and Status Around the World' (2007) Computer Society of India, 3.
697 Yu–Chen Chen and Jun–Yi Hseish 'Advancing E–Government: Comparing Taiwan and the United States' (2009) 69 Public Administration Review, 151–158.

and application of ICTs.'[698] Onuigbo et al describe it as the public sector's use of information and communication technologies with the aim of improving information and service delivery, encouraging citizens participation in decision making process and making government more accountable, transparent and effective.'[699]

From an aggregate of the definitions, e–governance is simply the use of digital platforms to exclusively regulate organisational decision–making process.

E–Governance and Data Protection

NITDA relies on e–governance in its preamble to the NDPR as its legislative basis for issuing the regulation, but it must be outrightly noted that e–governance is not necessarily synonymous with data protection, however the two concepts interrelate and power to regulate e–governance may or may not contemplate data protection. While it is conceded that personal data is key to e–governance since it forms the foundation upon which users are identified in most e–government platforms, its role in e–governance does not necessarily confer powers on regulators to issue guidelines on personal data protection.[700]

The relationship between e–governance and data protection may not be entirely denied since it is arguable that while e–governance is fixated on electronic service delivery, it raises data protection concerns and simultaneously develops practices that address

698 William Sheridan and Thomas Riley, William Sheridan and Thomas B. Riley, 'Comparing E–Government vs E–Governance; (eGov Monitor. Knowledge Asset Management Limited, London, 2006).
699 Richard Amaechi Onuigbo and Innocent Eme, 'Electronic Governance and Administration in Nigeria: Prospects and Challenges' (2015) 5(3) Arabian Journal of Business and Management Review, 18.
700 Ebenezer Agbozo, Daniel Alhassan and Kamen Spassour, 'Personal Data Privacy Barriers to E–Government Adoption, Implementation and Development in sub–Saharan Africa' in Electronic Governance and Open Society: Challenges in Eurasia (Springer International, New York, 2018).

privacy issues.[701] However, e–governance is the provision of information and services to citizens by government through digital platforms and data protection is the legal and technical means and procedure of securing citizens' personal information in the process, hence the two concepts are mutually exclusive and distinguishable. In other words, the power to make guidelines for e–governance does not necessarily translate into power to issue regulation for data protection under this limb merely because of the nexus between the two concepts.

On the other hand, when the meaning of 'guideline' as used in this provision is weighted against 'regulation' as used in the NDPR, NITDA's powers to make guidelines for e–governance appears to have been taken too far and interpreted to mean powers to issue regulation for data protection contrary to the unequivocal text of its enabling Act and cannons of interpretation of statutes.[702] More so, since guidelines are distinguishable from regulations in terms of their scope and binding effect, an agency ought not rely on its competence over one, to issue the other. In *Clementina Ogunniyi v Hon. Minister of Federal Capital Territory*, the Nigerian Court of Appeal defined guidelines as 'rules or instructions that are given by an official organization telling you how to do something, especially something difficult.'[703] In that case, the court was invited to determine the legal status of a particular set of approved guidelines for sale of Federal Government houses in Abuja to career civil servants as published in a public notice made by the Minister of the FCT pursuant to his delegated powers under section 18 of the FCT Act. Although the court declined to rule on the status of the guidelines since

701 Brendan van Alsenoy, Els Kindt and Jos Dumortier, 'Privacy and Data Protection Aspects of e–Government Identity Management' in Simone van der Hof, Marga M. Groothuis (eds) *Innovating Government*, (Springer International Publishing, New York, 2011).
702 Words used in statutes must be given their simple and ordinary meaning where they harbor no ambiguity. See PDP v INEC (1999) LPELR–24856 (SC), Croxford v Universal Insurance (1936)2 KB 253, 281, Oviawe v Integrated Rubber Products Nigeria Ltd (1997) 3 NWLR (Pt. 492) 126, 130.
703 (2014) LPELR–23164 (CA).

it was not relevant to the resolution of the appeal, the term was defined along the line of its nature as internal instructions within an organization.[704]

However, three years later, the Nigerian Supreme Court had the opportunity of ruling on the legal status of (policy) guidelines in *Comptroller General of Customs v Gusau*[705] to the effect that they do not constitute subsidiary legislation, hence guidelines are neither laws nor regulations.[706]Assuming e–governance under the limb considered embodies data protection, the wording of the provision is clear enough to show that it only contemplates guidelines, hence whatever is issued thereunder cannot have the same legal force as regulations which are legally binding subsidiary legislation.

b. Monitor use of electronic data interchange (EDI)

Again, NITDA Act provides no definition for 'electronic data interchange (EDIs)' as used in section 6(c) but the definition of 'electronic record' provided therein offers some insight as to what is contemplated by electronic data under the Act.[707]The term 'electronic data' refers to 'any original and any non–identified copies (whether non–identical because of notes made on copies or attachment, comments, annotations, marks, transmission notations, or highlighting of any kind) of mechanical, facsimile, electronic, magnetic, digital or other programs (whether private, commercial o work in progress), programming notes or

704 See also Olumide Babalola, Babalola's Law Dictionary of Judicially Defined Words and Phrases (2nd edn, Noetico Repertum, Lagos, 2019) 352.
705 (2017) LPELR–42081(SC).
706 See also Union Bank v Ifeoluwa Ent. Ltd (2007) 7 NWLR (Pt. 1032) 71 at 84 where the Court of Appeal had also held that guidelines are not subsidiary legislation, and they are without force of law.
707 Section 34 defines electronic record as 'data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer–generated micro fiche.'

instructions activity listings of electronic mail receipt.'[708]

Electronic Data Interchange (EDI) on the other hand, is the 'computer–to–computer exchange of structural business information' which could be electronic business documents as a structured exchange of business information between two or more firms using their computer systems.[709] Yunitarini et al clarify that EDIs are technologies used by world class organizations to communicate effectively with the business partners to improve their service–delivery.[710]

EDIs were historically created for businesses to reduce their operational costs of the preventable expensive process of entry of data and verification of paper–based documents, hence EDIs improve the accuracy of information by eliminating the regular errors characterized by the monotonous process of transcribing paper–based information to electronic platforms.[711]

Khazanchi defines them as the 'computer–to–computer interchange of business transactions that conforms to specified standards over a communications network that includes at least two partners.' He says these interactions include the interchange of common commercial information typically consisting of purchase orders, shipping notices, invoices, related acknowledgements, funds transfer with banks etc.[712]

708 Donald Burleson, 'A Comprehensive Definition of Electronic Data' <http://www.dba–oracle.com/t_electronic_data_definition.htm#:~:text=refers%20to%20any%20original%20and,commercial%2C%20or%20work%2Din%2D <www....> accessed 2 May 2021.
709 Hicham Amine and Abdelouab Mesnaoui, 'Electronic Data Interchange (EDI) in the Supply Chain: Impact on Customer Satisfaction' (2018) 4(6) Journal of Business Management, 15.
710 Rika Yunitarini Pratikto, Purnomo Budi Santoso and Sugiono Sugiono, 'A Literature Review of Electronic Data Interchange as Electronic Business Communication for Manufacturing' (2018) 9(4) Management and Production Engineering Review, 117–128.
711 Prem Premkumar, K. Ramamurthy and Sree Nilakanta, 'Implementation of Electronic Data Interchange: An Innovation Diffusion Perspective' (19941) 11(2) Journal of Management Information Systems, 157–186.
712 Deepak Khazanchi 'An Empirical Analysis of Benefits of Electronic Data Interchange (EDI) Implementation: Implications for New IT Implementation' (2002) 13(1) Journal of Small Business Strategy, 46.

In its simplest form, an EDI is an 'automated computer–computer transmission of standardized business, exchange of business documents/ transactions between partners.'[713]

From an aggregate of all the definitions, the common denomination of EDIs are 'computer to computer' 'business transactions' and 'business partners.[714] Hence, it is clear that, EDI is a communication technology used to facilitate organizational business goals especially between business partners and judging from the ordinary unambiguous wording of section 6(c), NITDA is empowered to monitor the use of EDI as a business solution technology especially with respect to the manner of executing inter–organizational transactions electronically in Nigeria. Invariably, NITDA is empowered under this provision to monitor the use of EDIs by businesses and this regulatory function is clearly different from data protection which concerns as rules that specifically regulate all or more stages in the processing of personal information.[715] It cannot however be conceived that NITDA's powers to monitor the use of EDIs is relatable to power to issue regulation on data protection as demonstrated in the table below:

713 Steve Walton and Ann S. Marucheck, 'The Relationship Between EDI and supplier Reliability?' (1997) 33(3) Information Journal of Purchasing and Material Management, 30–35.
714 Craig A. Hill and Gary D. Scudder, 'The Use of Electronic Data Interchange for Supply Chain Coordination in the Food Industry; (2002) 20 Journal of Operations Management, 375–387.
715 See Lee. A. Bygrave, Data Protection Law; Approaching its Rational, Logic and Limits (Kluwer Law International, 2002) 2). Data Protection has also been defined as a set of rules that was to protect the rights, freedoms and interests of individuals whose personal data are collected, stored, processed, disseminated, destructed, etc. See Maria Tzanou, 'Data Protection as a Fundamental Right, Next to Privacy? 'Reconstructing a Not so New Right' (2013) 3(2) International Data Privacy Law, 88–89.

EDIs	Data Protection
Technological device[716]	Rules/process/legal framework[717]
Applicable to business relations[718]	Applicable to all transactions (business, social, family etc)[719]
Computer to computer[720]	May involve computer or not.[721]
Electronic[722]	Hybrid (Paper–based and electronic[723]
Business data[724]	Personal data[725]
Between business partners[726]	Regulates processing of every natural person's data[727]
Structured format[728]	No specifications

716 Technology that enables business to business transactions. See 'Sriram Narayanan, Ann S. Marucheck and Robert B. Handfield, 'Electronic Data Interchange: Research Review and Future Directions' (2009) 40(1) Decision Sciences, 121.

717 Bygrave defines them as rules that specifically regulate all or more stages in the processing of personal information. See Lee A. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, New York, 2002) 2. Tzanou says data protection refers to 'a set of legal rules that aim to protect the rights, freedom and interests of individual whose personal data are collected, stored processed, discriminated, destructed etc.' See Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy?' (2013) 3(2) International Data Privacy Law, 88–99; Raphael Maurice Gellert, 'Understanding Data Protection as a Risk Regulation' (2015) 18(11) Journal of Internet Law, 3–15.

718 Sohel Ahmad & Roger G. Schroeder, 'The Impact of Electronic Data Interchange on Delivery Performance' (2009) 10(1) Production and Operations Management, 16–30.

719 The NDPR is applicable to all transactions involving exchange of personal data. See reg. 1.1(b).

720 Ramon O'Callaghan and Jon A. Turner, 'Electronic Data Interchange Concepts and Issue' in *EDI in Europe*, H. Krcmar, N. Bjsrn–Andersen, and R. O'Callaghan, (eds) (John Wiley & Son, 1995) 1.

721 Stefan Fenz, Johannes Heurix, and Thomas Neubauer, 'Recognition and Privacy Preservation of Paper–Based Health Records' (2012) 180 Studies in Health Technology & Informatics, 751.

722 Paula Swatman and Craig Parker, 'Traditional EDI and Supply Chain Management' (2002) University of Deakin, School Working Papers Series 2002 SWP 2002/55, 1.

723 Dragan Savić and Mladen Veinović, 'Challenges Of General Data Protection Regulation (GDPR)' International Scientific Conference On Information Technology And Data Related Research, (Sinteza, 2018) 23, 27.

724 Rika Yunitarini Pratikto, Purnomo Budi Santoso and Sugiono Sugiono, 'A Literature Review of Electronic Data Interchange as Electronic Business Communication for Manufacturing' (2018) 9(4) Management and Production Engineering Review, 117–128.

725 Renata M. de Carvalho, Camillo Del Prete, Yod Samuel Martin, Rosa M. Araujo Rivero, Melek Önen, Francesco Paolo Schiavo, Ángel Cuevas Rumín, Haralambos Mouratidis, Juan C. Yelmo, Maria N. Koukovini, 'Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects' (2020) 1 SN Computer Science, 217.

726 Narayanan et al (n. 85) 122.

727

728 Yunitarini et al (n. 92).

Two–way communication[729]	There may not be communication as the data subject may not even be aware of processing of his personal data.[730]
Facilitates exchange of business documents[731]	Safeguards personal data in all environments (businesses, social and all others) [732]

Ultimately under this limb, the NITDA Act is fixated on other forms of electronic communications transactions as an alternative to paper–based methods, even when one concedes vires to regulate data protection in favour of NITDA, its enabling Act's reference is restricted to electronic communications and that takes away the power to regulate all kinds of data processing. It must also be ultimately emphasized that data protection is not even about communication but management of personal data as it concerns processing of personal information, which is not even communicated in most cases and these facts somewhat rob NITDA of any jurisdiction to regulate data protection as a whole.

Functions and powers under the NDPR

Under the NDPR, NITDA is not expressly conferred with powers to perform all functions performed by other DPAs elsewhere.[733]

729 Izak Benbasat, Paul Chwelos, Albert S. Dexter, and Clive D.Wrigley, 'Electronic Data Interchange' (2003) Encyclopaedia of Information Systems, 47–55.

730 Yvonne McDermott, 'Conceptualising the Right to Data Protection in an Era of Big Data' (2017) Big Data & Society, 1, 3.

731 Collin Ramdeen Jocelina Santos & Hyun Kyung Chatfield, 'EDI and the Internet in the E–Business Era' (2009) 10(3) International Journal of Hospitality & Tourism Administration, 270.

732 Radi Romansky, 'Social Media and Personal Data Protection' (2014) 4 International Journal on Information Technologies & Security, 65, 75.

733 DPAs are meant to provide 'expert advice' on data protection matters, issue guidance notes and inform the public on their rights and obligations under the relevant data protection laws. While NITDA may claim to perform some of these roles, the NDPR is not clear on them. For more reading on roles of DPAs, see Peter Hustinx, 'The Role of Data Protection Authorities' in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds) *Reinventing Data Protection?* (Springer International Publishing, Dordrecht, 2009) 133.

More so, there is no dedicated provision under the NDPR on the functions, duties and powers of NITDA which agency is listed as one of the DPAs since the definition of 'relevant authorities'[734] groups NITDA alongside other sectoral regulators especially as some other functions are reserved for the 'supervisory authorities' and 'relevant authorities' under the regulation.[735] However, without prejudice to reductionist arguments on the propriety of NITDA's issuance of the NDPR pursuant to its enabling Act, the NDPR envisages the agency as one of the DPAs in Nigeria with some clear–cut functions and role–playing in the country's data protection ecosystem.[736]

Decision on adequacy level.

One of the paramount objectives of data protection laws is the development of mechanisms to ease the free flow of personal data within countries and international organisations without prejudice to the rights and freedoms of data subjects and with the assurance of commensurate and equivalent level of protection across board.[737]

This requirement for cross border data processing was introduced by the EU Data Protection Directive 95/46/EC that, 'member states shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the Directive, the third country in question

734 See NDPR, reg. 1.3(xxiv).
735 See NDPR, reg. 2.11(d) and 4.3.
736 The World Bank notes in its Digital Economy Diagnostic Report on Nigeria that, 'the function of the supervisory authority for data protection is unassigned' < http://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria–Digital–Economy–Diagnostic–Report.pdf> accessed 15 May 2021.
737 Spiros Simitis, 'From the Market to the Polis: The EU Data Protection Directive on the Protection of Personal Data?' (1995) 80 (3) Iowa Law Review, 445–469.

ensures an adequate level of protection.'[738] Under European data protection legal regime, it is the European Commission that makes the adequacy decision and implements same by means of an Implementation Act.[739] The GDPR seeks to maintain a balance between the necessity of transfer of data for international trade as well as affording protection to data subjects over their personal data are processed in the course of such cross border transactions. The requirement provides extraterritorial protection for data even after its transfer out of EU coverage in cases of adequate data protection or in other cases subject to certain exceptions.[740]

The European jurisprudence on data protection however experienced a shift when in July 2020, the CJEU handed down a landmark decision in *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems (Schrems II)*[741]where the court found that the US Privacy Shield[742]did not pass the adequacy test under European data protection law.[743] The court's decision has however been viewed by some commentators, especially in the US, as imbalanced and lacking in protection in some specialised cases[744]while Tzanou concludes that although the decision was

738 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, art. 25(1); see also Jennifer Stoddart, Benny Chan and Yann Joly, 'The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research, (2016) 44(1) The Journal of Law Medicine and Ethics, 1; see also article 26 of the EU Data Protection Directive which provides exceptions for situations where data subject consents or transfer is necessary to perform a contract or in public interest etc.

739 de Carvalho et al (n. 94) 231.

740 GDPR, art 45(3): see also Julian Wagner, 'The Transfer of Personal Data to Third Countries Under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?' (2018)8(4) International Data Privacy Law, 318, 320.

741 C–311/18

742 A data protection framework devised by the US Government to replace the Safe Harbour which was also earlier invalidated by the CJEU in Maximillian Schrems v Data Protection Commissioner Case C–362/14 in 2015) as a mechanism for American–based companies to transfer personal data of EU residents to the United States while ensuring compliance with EU data protection rules.

743 See Dara Hallinan, Alexander Bernier, Anne Cambon–Thomsen, Francis P. Crawley, Diana Dimitrova, Claudia Bauzer Medeiros, Gustav Nilsonne, Simon Parker, Brian Pickering and Stéphanie Rennes, 'International transfers of personal data for health research following Schrems II: a Problem in need of a Solution' (2020) European Journal of Human Genetics, 1.

744 See Stewart Baker, 'How Can the U.S. Respond to Schrems II?', (2020) www.lawfareblog.com/how–can–us–respond–schrems–ii > accessed 23 May 2021; Peter Swire, '"Schrems II" backs the European legal regime into a corner — How can it get out?' (2020) International Association of Privacy Professionals (IAPP) www.iapp.org/news/a/schrems–ii–backs–the–european–legal–regime–into–a–corner–how–can–it–get–out > accessed 23 May 2021.

comprehensible, it was devoid of clear cut conditions for internal and external extraterritoriality.[745]

Conversely, under the NDPR, NITDA makes decisions on whether a country or foreign organisation ensures adequate level of data protection.[746] However, unlike the detailed rules in GDPR, the NDPR also does not make elaborate provision on the parameters and modalities of this decision–making powers but the Implementation Framework issued pursuant to the NDPR provides a bit of clarity on adequacy decisions as issued by NITDA in favour of countries in conjunction with the office of the Attorney General of the Federation.[747] NITDA appears to have however made adequacy decisions in favour of all African Countries–signatories to the Malabo Convention;[748] all European Union and European Economic Area countries; Algeria, Argentina, Bahram, Benin (repeated even though it is a signatory to the Malabo convention), Brazil, Ghana, Mauritius, South Africa, Togo (signatory) Tunisia (signatory), Canada, Cape Verde, China, Cyprus, Israel, Japan, Philippines, Singapore, South Korea, Faroe Islands, Isle of Man, Jersey, Liechtenstein, Switzerland, Kenya, United States of America, Guernsey, Japan, Hong Kong, Malaysia, Mauritius, Qatar, Taiwan, Turkey, United Arab Emirates, India and Uruguay. [749]

While it is clear from the NDPR and its Implementation Framework that adequacy decision is reached by NITDA in consideration of 'legal agreements' and directives of the office of Attorney General of the Federation, the parameters and factors for reaching such

745 Maria Tzanou, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in Federico Fabbrini, Edoardo Celeste and John Quinn, (eds) , *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty,* (Hart Publishing, London, 2020) 99.
746 NDPR, reg.2.11(a).
747 NDPR Implementation Framework, November 2020, clause 14.2.
748 Benin, Chad, Comoros Congo, Ghana, Guinea–Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome, & Principe, Togo, Tunisia and Zambia. Ironically, Nigeria is not even a signatory to the Malabo Convention, and this constitutes an indictment on its own adequacy status.
749 See NDPR Implementation Framework, annexure C.

decisions are still undisclosed in the NDPR.[750]

Receiving information on refusal of Data Subject Access Request (DSAR)

Data Subjects Access Request (DSAR) springs from the data subjects' right to be informed on processing activities performed on his/her personal data.[751] It is one of the most fundamental data protection rights which guarantees data subjects' access to information from data controllers on processing activities on their personal data in such controllers' possession.[752]This right plays a vital role in enhancing data subjects' control over their personal data on one hand and it also enables them monitor data controllers' compliance with data protection legislation.[753]

Data controllers under the NDPR are duty–bound to provide data subjects with information relating to processing of their data in a concise transparent, intelligible and easily accessible form.[754] However, where a controller refuses DSAR on any of the grounds provided under the regulation, it must copy NITDA in the letter of refusal through a dedicated channel for that purpose[755] thereby underscoring the regulatory role played by NITDA in ensuring the respect of DSAR and ascertaining the propriety of derogation in deserving cases.

750 The factors for consideration are well detailed under the GDPR where, to determine adequacy, the European Commission is required to consider rule of law, respect for human right and other factors in the country or organisation concerned. See Art. 45 (2) (a)–(c) and recital 104; see also Laura Drechsler, 'Comparing LED and GDPR Adequacy: One Standard Two Systems' (2020) 1(2) Global Privacy Law Review, 93–103.
751 Paul Buckle, 'Data Subject Access Request and Beneficiaries' Right to Information' (2019) 25(3) Trusts and Trustees, 328–342.
752 Luca Bufaleiri, Massimo La Morgia, Alessandro Mei, & Julinda Stufa. 'GDPR: When the Rights to Access Personal Data Becomes a Threat' (2020) IEEE, 1.
753 Jef Ausloos, Rene Mahieu and Micheal Veale 'Getting Data Subjects Rights Right. A Submission to the European Data Protection Board from International Data Rights Academics to Inform Regulatory Guidance' (2019) 10 JIPITEC, 283.
754 NDPR, reg 3.1(1).
755 NDPR, reg. 3.1 (3)(b).

Registration and Licensing of Data Protection Compliance Organizations (DPCOs)

The NDPR creates an arguably unique licensing regime for a special class of enforcement agents which are authorised to perform certain regulatory roles on behalf of NITDA.[756] It is worthy of note that, a similar provision exists in article 41 of the GDPR which empowers supervisory authorities in EU member states to accredit competent bodies with requisite expertise in data protection to perform the envisaged functions.[757] This power sees NITDA delegate some of its regulatory functions to licensed DPCOs especially to monitor compliance, audit data controllers, data processing activities, conduct training and provide consulting services to controllers and processors.

d. Receipt of audit reports

In European law, supervisory authorities carry out investigation in the mould of data protection audits[758] but in Nigeria, NITDA is duty–bound to receive annual data audits from data controllers effectively showing their transparency and legality of their data processing activities. Regulation 4.17 NDPR mandates that, 'on annual basis, a data controller who processed the personal data of more than 2000 data subjects in a period of 12 months shall, not later than the 15th of March of the following year, submit a summary of its data protection audit to the agency containing information as specified in reg. 4.1(5) NDPR.[759]

756 NDPR, reg. 4.1(4).
757 Eric Lachaud, 'What GDPR Tells About Certification' (2020) 38 Computer Law and Security Review, 1.
758 Art 58(1) and (6) GDPR), see also Martin Brodin, 'A Framework for GDPR Compliance for small and medium sized Enterprises (2019) 4 European Journal for Security Research, 243–264.
759 The audit must contain information on: (a) personal data collected from employees or other data subjects; (b) purpose of collection; (c) privacy notice (d) DSAR; (e) method for obtaining consent (f) data protection practices and procedure etc.

Independence of NITDA

Issues bordering on independence and impartiality of national DPAs superficially appear simple but they have been regarded as complex and multifaceted. To ascertain independence of DPAs, Gilardi has devised some factors indicating independence and impartiality thus: (a) agency's head and board's status; (b) relationship with government and parliament; (c) financial and organizational autonomy; (d) delegated regulatory competencies.[760]

European law stipulates that DPAs shall act with complete independence in the performance of their statutory duties[761] and the GDPR expects that, supervisory authorities shall ensure that, their members must not take instructions from anybody, their members must refrain from incompatible duties or occupation during the course of their term, members must behave with integrity and discretion after their term regarding accepting appointments, DPAs must be provided with adequate, human, technical and financial resources but the DPA shall not be subject to financial control which shall all affect its independence.[762]

a. *NITDA's head and board's status*

The agency's affairs are statutory directed by a board which has overall control over it.[763] The board is appointed by the country's President subject to the recommendation of the minister responsible for science and technology[764] and the board's secretary

760 Fabrizio Gilardi, 'Policy Credibility and Delegation to Independent Regulatory Agencies: A Comparative Empirical Analysis' (2002) 9 Journal of European Public Policy, 873–893.
761 Philip Schutz, 'Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective' (2011) 7th Prime Life International Summer School, Trento, Italy, 45–58.
762 GDPR, art. 47; see also European Union Agency for Fundamental Rights, 'Elements of Independence of the Data Protection Authorities in the EU' <https://www.asktheeu.org/en/request/2398/response/9765/attach/3/21.FRA%20Focus%20Data%20protection%20authorities%20independence%20funding%20and%20staffing%20ATTACHMENT%20FRA%202013%20Focus%20DPA.pdf > accessed 29 April 2021.
763 NITDA Act, s.2(1) and (2).
764 NITDA Act, s.2(3).

doubles as the agency's director–general and chief executive/ accounting officer responsible for the day–to–day administration of the agency.[765] In this situation where the board has a chairman but the chief executive/ director general oversees the day–to day–affairs of the agency one then wonders who qualifies as the head of the agency between the former and latter.

Differentiating the two offices, Glick[766] identified the following roles played by chief executive: informational role,[767] interpersonal role,[768]decisional role,[769] operational,[770] strategic role,[771] diplomacy role[772] and then concludes that, the CEO is the most significant office that leads organizations.

On the significance of the board chair in corporate governance, the leadership role of a chair depends on the CEO, but they are often times assigned with the operational responsibilities over the business management.[773] While the chair acts like the 'consultant and coach' to the chief executive, by monitoring and supervising the CEO and this gives an impression that the latter is subservient to the former.[774] However argue that while the CEO manages an organization's everyday administration and strategies, the chair,

765 NITDA Act, s.2 (2) (f) and 8(1).
766 Margaret B. Glick, 'The Role of Chief Executive Officer' (2011) 13(2) Advances in Developing Human Resources, 172.
767 Sune Carlson, *Executive Behaviour. A Study and the Working Method of Managing Directors* (Stromberg, Stockholm, 1951).
768 Henry Mintzberg, *The Nature of Managerial Work* (Harper Row, New York, 1973).
769 Stefan Tergblad 'Is there a New Managerial Work? A Comparison with Henry Mintzberg's Classic Study 30 Years Later' (2006) 43 Journal of Management Studies, 143.
770 Wendy Bodwell & Thomas Chermack 'Organizational Ambidexterity: Integrating Deliberate Emergent Strategy with Scenario Planning, Technological Forecasting and Social Change, 77.
771 Zahra Ramezani et al, 'Use of Mintzberg's Model of Managerial Roles to Evaluate Sports Federations Managers of Iran' (2011) 10(5) Middle East Journal of Scientific Research, 559–564.
772 A.G Lafley, 'What only the CEO Can Do' (2009) 87(5) Harvard Business Law Review, 54–62.
773 Anup Banerjee, Mathias Nordquist and Karin Hellerstedt, 'The Role of the Board Chair–A Literature Review and Suggestion for Future Research' (2020) 28 Corporate Governance International Review, 372–405.
774 Gideon Chitayat, 'Working Relationships Between Chairman of the Board of Directors and the CEOs' (1984) 24 Management International Review, 65–70; Adrian Cadbury *Report of the Committee on the Financial Aspects of Corporate Governance* (Gee ,London, 1992); Andrew Kakabadse and Nada Kakabadse, 'Chairman and Chief Executive Officer (CEO): That Sacred and secret Relationship' (2006) 25(2) Journal of Management Development, 150.

through the board, leads and monitors the top management to ensure optimal efficiency.[775] On his perceived pre–eminence of the chairman over the CEO, Jensen notes that, 'the role of the Chairman of the board is to run board meetings and oversee the process of hiring, firing, evaluating, and compensating the CEO. Clearly the CEO cannot perform his function apart from his or her personal interest without the direction of an independent leader, hence, it is much more difficult for the board to perform its critical function.[776]

Under NITDA Act, the chairman appears to be the head of the agency since he leads the board that oversees the agency's general affairs but with respect to their independence, the same conditions apply to both chairman and chief executive in terms of their appointment, remuneration, term of office, vacation of office[777] they are both appointed by the President on the recommendation of minister of science and technology,[778] paid such emoluments, allowances and benefits fixed by Federal government[779] and their terms fixed for four years but renewable.[780]

From the express provisions of NITDA Act, it is seen that the head of the agency (whether the chairman or chief executive (director general) is an appointee of the President of the Nigeria and continuance in that office is at the President's pleasure as he can remove such officer on the recommendation of the minister alone[781] or where the President is satisfied that the officer is no

775 loannis Antoniadis et al, *Separating the Roles of CEO and Chairman of the Board. The Case of Greek Listed Firms in Accounting and Finance in Transition* (vol. 11, Greenwich University Press, London, 2005).
776 Michael C. Jensen, 'The Modern Industrial Revolution, Exit and the Failure of Internal Control Systems' (1993)48 Journal of Finance, 831–880.
777 NITDA Act, s.4.
778 NITDA Act, s.2(3).
779 NITDA Act, s. 5.
780 NITDA Act, s.3.
781 See NITDA Act, s. 11.

longer fit for the job.[782]

The President's overbearing stance on the appointment of NITDA's heads and their continuation in office confirms the unsavoury statutory dependence of such appointees on their appointors, they derive their official livelihood and sustenance from their appointor, to whom they explicably owe their allegiance but to the detriment of the organization which ships they ought to steady with a measure of discretion. The board members also suffer same fate as the chair and chief executive, they are not only fastened to President and his minister's apron strings, but they are also hired and fired at the pleasure of the President and his cabinet without any form of check in the enabling Act. Ultimately, NITDA cannot be regarded as an independent agency if its heads (understandably) go cap in hands to their statutory benefactor as designed by the agency's enabling Act.

b. Relationship with government and parliament

It is inarguable that a close, undefined relationship between the government and DPAs, erodes an expectation and/or situation of complete independence. In *European Commission v Federal Republic of Germany*,[783] the European Court of Justice found that the government's establishment of DPAs to monitor data processing activities of some private bodies which competed with public bodies negated the assurance of complete independence. The court conclusively declared that 'by making the authorities responsible for monitoring the processing of personal data … subject to State scrutiny, and by thus incorrectly transposing the requirement that those authorities perform their functions 'with

782 Section 4(1) (f) NITDA Act. Note that there are no statutory parameters for this subjective satisfaction on the part of the president and this further pronounces a completed dependence on the office of the president.
783 Case C–518/07. See also Olumide Babalola, Casebook on Data Protection (Noetico Repertum, Lagos, 2020) 582.

complete independence', the Federal Republic of Germany failed to fulfil its obligations…"[784]

Under its enabling Act, NITDA's board members' relationship with the government is found in their appointment, government's review of staff remuneration,[785] its advice to the federal government on certain matters,[786] its reports to the minister of science and technology[787] and its taking of directives from the minister.[788] With NITDA's current setup that sees it operate under a ministry while reporting directly to the minister in charge coupled with its varying description as an 'implementing arm'[789] of a federal ministry, its relationship with the government beclouds any sense of independence the agency may allude to.

c. Financial and Organisational autonomy

Financial autonomy consists of income autonomy and expenditure autonomy.[790] It is the 'power to control finance, manage it and allocate resources to strategic place.'[791] To perform their statutory functions without government's influence supervisory authorities ought to enjoy some measure of financial autonomy, i.e, they should have their source of income/funding, independent budget that is directly funded from the national budget, (lump sum budgetary allocation), and freedom to use budgetary allocation in

784 Para 58 of the judgment.
785 S. 8(5).
786 Matter listed in the second schedule of the Act included creation of organizational departments, annual business plan etc.
787 S. 23.
788 However, by a political arrangement, contrary to the express provision of section 23 of NITDA Act, the agency was moved to the ministry of communications and digital economy at the expense of federal ministry of science and technology. See https://nitda.gov.ng/mandate/ > accessed 2 May 2021.
789 World Bank 2006, Information and Communications for Development Global Trends and Policies < https://openknowledge.worldbank.org/handle/10986/6967> accessed 14 May 2021.
790 Lasse Oulasvirta and Maciej Turala, 'Financial Autonomy and Consistency of Central Government Policy Towards Lord Governments' (2009) 75 International Review of Administrative Sciences, 311.
791 Kehinde Osakede, Samuel Ijimakinwa and Taiwo Adesanya, 'Local Government Financial Autonomy in Nigeria: An Empirical Analysis' (2016) 5(11) Kuwait Chapter of Arabian Journal of Business and Management Review 24, 29.

the exercise of their statutory duties/powers etc. [792] The concept of financial autonomy lacks a definitional precision[793] but it has been defined as the 'ability of institutions to manage their financial affairs independently without external influence.'[794] Chapman says fiscal autonomy is a body's ability to increase revenue and decide how to expend same.[795] Ebohon et al view it from the perspective of independence of political structures and institution from the lower level of government[796] and it is worthy of note that, another factor which underscores financial autonomy is budgetary independence i.e. is the agent funded by other supervised entities, does it submit its budget directly to government or a ministry thereunder, does it enjoy autonomy in defining salaries and salary structures of stuff, can the agency autonomously hire staff, can the agency define its internal organisational structure?.[797] Nothing in its enabling Act empowers NITDA to draw an independent budget for the approval of parliament, rather it gets it budgetary allocation through the ministry under which it operates.[798]

In the same vein, the Act recognises a National Information Technology Development Fund which may be expended on staff salaries, payment of emoluments etc but with the federal government's institution of the Treasury Single Account,[799] the practicality of such expenditure from the fund may no longer be

792 Carl–Johan Lindgren and D.F.I Folkerts–Landau, 'Supervisory Oversight' in Towards a Framework for Financial Stability (International Monetary Fund, 1998).
793 Adrian Scutariu and Petrosula Scutariu, 'The Lines Between Financial Autonomy and Local Development. The Case of Romania' (2015) 32 Procedia Economic & Finance, 542.
794 Slavica Petkovska, 'An Analysis of financial Autonomy in Macedonian Higher Education' (Master's Thesis, University of Avaro, 2011).
795 Jeffery I. Chapman, 'Local Government, Fiscal Autonomy and Fiscal Stress: The Case of California' (1999) Lincoln Institute of Land Working Paper.
796 S.I. Ebohon, Osa Osemwuta and Phillip Agbebuku 'Autonomy and Local Capacity. An Analysis of the Performance Profile of Edo State Local Government Councils' (2011) 6(3) 16 Mendwell Journals, The Social Science, 235–236.
797 Donato Masciandaro, Mare Quintyn and Michael Taylor, 'Financial Supervisory Independence and Accountability–Exploring the Determinant' (2008) IMF Working Paper, 1, 5.
798 NITDA Act, s. 20(a).
799 NITDA Act, s. 12(1) and 21. See also Godwin Oyedokun, 'The Imperative of Treasury Single Account (TSA) in Nigeria' (2016) < https://www.researchgate.net/publication/318000438_Imperative_of_Treasury_Single_Account_TSA_in_Nigeria> accessed 14 May 2021.

possible.

On the whole, NITDA's independence is plagued by its relationship with its principal ministry, the President's power to hire and fire its board members at will, its lack of independent budget and ultimately circumstances surrounding its creation as an agency for the implementation of the ministry's policies which do not expressly include data protection, hence data protection does not represent its principal mandate.[800]

800 The agency's eight priority areas are: developmental regulations, digital literacy and skills, solid infrastructure, service infrastructure, digital services development and promotion, software infrastructure, digital society and emerging technologies and indigenous content development and adoption. There is not one department or unit within the agency dedicated to data protection in the agency's service charter. (see NITDA Service Charter, (3rd edition 2021) < https://nitda.gov.ng/wp–content/uploads/2021/03/nitda1.pdf> accessed 12 May 2021.

CHAPTER EIGHTEEN

The enforcement of data protection

By their very nature, DPAs are entitled to resources which necessarily aid their performance of duties and protection of data subjects' rights but inadequate or inefficient enforcement mechanisms are inimical to the growth of data protection legislation in any country.[801] The NDPR creates a peculiar enforcement and compliance mechanism which sees a quartet of players aid NITDA in its regulatory functions around data protection:

- Data Protection Compliance Organisation (DPCO)
- Data Protection Officer (DPO)
- The Police
- The Attorney General of the Federation (AGF), and
- The Administration Redress Panel (ARP)

Data Protection Compliance Organization (DPCO)

This is arguably a novel invention[802] of NDPR, defined as 'any entity duly licenced by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with the NDPC or any foreign data protection law or regulation having effect in Nigeria.'[803] Unlike NITDA's licenced DPCOs, article 41 of the GDPR empowers

801 Muli David Tovi and Mutuu Nicholas Muthama, 'Addressing the Challenges of Data Protection in Developing Countries' (2013) 1(1) European Journal of Computer Science and Information Technology, 1–9.
802 Novel in the sense of its name and nature as existing licenced Firms rather than bodies specifically created for that purpose as contemplated under European law.
803 Reg. 1.3 (xiii)

supervisory authorities in the EU member states to 'accredit' competent bodies with demonstrable level of expertise to perform functions specified in relevant code of conduct.[804] The GDPR does not contemplate a multitude of monitoring bodies (per sector) which will be accredited by codes of conduct but the NDPR is empowered to licence many Firms to provide certain audit and remedial services envisaged by NDPR. The rationale for licencing DPCOs under the Nigerian ecosystem is found in the NDPR's reaction to the population of data controllers and diversity of the Nigerian economy. This makes it almost impossible for NITDA to unilaterally monitor and ensure compliance with the NDPR, hence its designation of DPCOs to, in the course of their audit exercises, evaluate the status of data controllers' compliance, appraise adequacy of protection offered to data subjects, identify current and potential non–compliance and draw out remedial and implementation plans.[805] The DPCOs are licenced to act on behalf of NITDA to ensure compliance with the NDPR[806] while the Implementation Framework however elaborates on their functions; thus: (a) evaluation of data controllers compliance status, (b) appraisal of data protection rights of data subject, (c) assessment of management level of awareness, identification of potential non–compliance and drawing up remedial plans.[807]

Data Protection Officer (DPO)

Although the GDPR expressly makes it an obligation for controllers within its scope to designate DPOs especially in EU member states, some national data protection laws had created the office long before the adoption of the regulation, hence it is not a particularly

804 Eric Lachaud 'Adhering to GDPR Codes of Conduct: A Possible Option for SMEs to GDPR Certification' (2019) 3(1) Journal of Data Protection & Privacy, 48–68.
805 Olumide Babalola, 'A Bird's Eye Rundown on Nigeria's Data Protection Legal and Institutional Model' (2021) 12(2) Gravitas Law Review of Business & Property Law, 27.
806 NDPR, reg. 4.1(4).
807 NDPR Implementation Framework 2020, clause 6.5.

new phenomenon in Europe.[808]

The office is not particularly defined in most data protection legislation, but by the nature of their work, they are simply, independent privacy or data protection professionals, designated, appointed, or recruited to ensure organisational compliance with data protection laws by internally educating and advising data controllers on their obligations under the relevant laws on one hand while acting as a liaising contact for the data protection authority on the other hand.

Ordinarily, a DPO ought to be knowledgeable in data protection, independent, equipped with adequate resources, immune from organisational influence and assured of job security while performing his/her role, there are no universally prescribed professional qualifications for occupants of the office.[809]

Under the NDPR, every data controller is duty–bound to designate a DPO to ensure organisational compliance with data protection laws and regulations and such organisations are duty–bound to ensure capacity building for the DPO which role, like obtainable under the GDPR, can be outsourced to an organisation or a person.[810]

The Police

Most data protection laws criminalize certain dealings with personal data e.g, privacy offences. For example, the English

808 The French national data protection law no. 78–17 enacted in 1978 had a provision on the office, see also art. 17 of the Belgian 1982 Act, art. 1 of Bulgarian Ordinance No.1 of 2013, section 30 of the Estonian Personal Data Protection Act of 2007 and section 24 of the Hungarian Act CXII etc.
809 GDPR simply provides that designation should be on the basis of professional qualities and expert knowledge of the field. See also Paul Lambert, *The Data Protection Officer: Profession, Rules and Role* (Auerbach Publications, Boca Raton, 2017) 20; European Data Protection Supervisor, 'Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001' (2005) https://edps.europa.eu/sites/edp/files/publication/05–11–28_dpo_paper_en.pdf accessed 1 July 2021.
810 NDPR, reg. 4.1(2) and (3), GDPR, art. 36(6).

Data Protection Act prohibits and punishes unlawful obtaining of personal data, re–identification of de–identified personal data, unlawful alteration of personal data.[811] In the same vien, the NDPR assigns NITDA with the responsibility of ensuring compliance with NDPR and alludes to the criminal nature of breach of data privacy rights which renders violators to criminal liability.[812] While the regulation does not expressly list offences and their punishment, it equates the breach of its provisions with that of NITDA Act and for the avoidance of doubt, sections 17 and 18 provide imprisonment and fines for violation of any of the provision of NITDA Act. Although the notion of imposition of fines for violation data protection rights connotes administrative rather than criminal sanctions, it is apparent that, the provision of the NDPR on fines conflicts with sections 17 and 18 of NITDA Act on the amount payable by violators; while NDPR prescribes between N2 Million and N10 Million, the Act imposes between N200, 000 and N500, 000. Since the Act is the principal legislation, its provision ordinarily overrides that of the regulation made pursuant to it. In *Odeleye v Efunuga,*[813] the Supreme Court ruled that a subsidiary legislation must be in conformity with the terms of its enabling law,[814] hence the fines provided under the NDPR will give way to the provision of the Act in that regard.

Without prejudice to NITDA's investigatory powers over data protection rights violation, the Nigeria police is assigned the statutory duty of investigating crime especially for the purpose of prosecution and in this case, violation of NDPR provisions. While the GDPR does not expressly contemplate criminal liability, member states have transposed its provision to create data

811 English Data Protection Act, 2018, ss. 170–173.
812 NDPR, reg. 2.10.
813 (1990) LPELR–2208(SC).
814 See also See Din v. AG Fed. (1988) 4 NWLR (Pt.87) 147 @ 154; Macfisheries (Wholesale & Retail) Ltd. v. Coventry Corporation (1957) 3 All E.R. 299 @ 302 and Kaycee (Nig.) Ltd. v. Prompt Shipping Corporation & Anor (1986) 1 NWLR (Pt.15) 180.

protection offences in their respective laws.[815] Under the NPDR, the police is expected to play a vital role in investigating privacy offences especially when referred by NITDA to establish a prima facie case for prosecution.

The Attorney General of the Federation (AGF)

The office of Attorney General is a common law idea which connoted a general agent of representation of the Crown. The office of Attorney General (of the federation) in Nigeria is although constitutionally recognized, it is a common law office that was historically created as a general agent or representative of the Crown.[816] Mba notes that, 'the pre–eminent position of the Attorney General under the constitution as the chief law officer of the state, generally as chief legal adviser to the state and specifically in all court proceedings to which the state is a party is a common law feature of constitution of commonwealth countries. In my jurisdiction including Nigeria, the constitution confers the office with similar powers to the common law prerogatives for exercise ultimate control over prosecutions.'[817]

By virtue of regulation 2.11 NDPR, NITDA regulates international transfer of personal data under the supervision of the AGF which office is duty bound to consider legal systems and respect for rule of law in the countries concerned, among other factors before coming to a conclusion on the adequate level of data protection in those countries.[818] Under European law, the European Commission plays the role played by the AGF in Nigeria's data protection

815 Gary Brooks, 'Data Protection: Tougher Penalties for Data Protection Offenses' (2007) 9(1) Journal of Direct, Data and Digital Marketing Practice, 86.
816 Charles Uwensuyi Edosomwan, 'Power of the Nigeria Attorney General in Perspective' in Olumide Babalola (ed) *The Attorney General: Chronicles and Perspectives* (Grace Info Tech Ltd, Lagos, 2013) 30.
817 Osita Mba, 'Judicial Review of the Prosecutorial Powers of the Attorney General in England and Wales and Nigeria: An imperative of the Rule of law' in Olumide Babalola (ed) *The Attorney General: Chronicles and Perspectives* (Grace Info Tech Ltd, Lagos, 2013) 50.
818 Reg 2.11 (a).

ecosystem but does more by coordinating transfer requests in conjunction with NITDA pursuant to the white list of countries with adequate level of data protection as drawn by the latter.[819]

Outside the AGF's prosecutorial powers, the NDPR has been conferred additional power on the office to supervise NITDA in the regulation of international transfer of personal data of natural persons subject to the NDPR but the regulation does not elaborate on the applicable procedure.[820] But the AGF must consider the legal system and respect for the rule of law & human rights in the country concerned among other factors[821] while it is NITDA that actually makes decisions on the adequacy level of data protection in such countries.[822]

Administrative Redress Panel (ARP)

Sometimes, court–based dispute resolution systems fail to provide the anticipated reprieve to victims, hence their resort to other internal complaint handling mechanisms.[823] Nigeria's justice system is characteristically described with its snail speed, from police investigation to court decisions, litigants are clearly becoming disillusioned by the system's counter–productivity and thereby tilting in favour of alternative dispute resolution mechanisms. In addition to data subjects' right to seek redress in court, NITDA ought to set up the ARP to investigate allegations of violation of data subjects' rights and to issue administrative

819 The NDPR does not make provision for the Whitelist, but its Implementation Framework does. see clause 7.2 and annexure C.
820 Procedure for enforcing privacy rights is a distinguishing feature of data protection as opposed to privacy. See Norbeto Nuno Gomes de Andrade, *Data Protection, Privacy and Identity; distinguishing Concepts and Articulating Rights in Privacy and identity Management for Life* (1st ed, Springer 2011) 96.
821 NDPR, reg. 2.11.
822 The AGF, in its supervisory role may however prohibit transfer to such countries in the event that their data protection legal framework is in adequate. See NDPR Implementation Framework, clause 14.2.
823 'The Law Commission, 'Administrative Redress: Public Bodies and the Citizen' (2008) Constitution Paper No. 187, 7.

orders in deserving cases.[824]

The Nigerian Federal High Court in *Digital Rights Lawyers Initiative v. Unity Bank Plc*[825] however impliedly interpreted 'without prejudice' found in regulation 4.2 (1) NDPR as a constituting condition precedent which a data subjects must fulfil before approaching the court. In other words, the court ruled that data subjects must seek redress before the ARP before approaching the court.

The court's decision is rather curious for two reasons: first, the phrase 'without prejudice' has been held by the Nigerian appellate courts in a plethora of cases to mean 'notwithstanding.'[826] Secondly, the ARP can only issue administrative orders and fines payable to government confers but not compensatory damages to victims of data breach unlike what is obtainable under the GDPR.[827] The court failed to appreciate the difference between administrative fines which the ARP is empowered to issue and compensatory damages which can only be issued by the courts.

The GDPR makes provision for compensatory damages under article 82 and administrative fines under article 83 but the NDPR is silent on damages to victims of data breaches and after two years of the NDPR, the ARP had not been set up but NITDA has issued two reported administrative fines in the last twelve months for data breach, yet nothing was said about compensation to the victims thereby confirming the assertion that NITDA together

824 NDPR, reg. 4.2.
825 Suit No. FHC/AB/CS/85/2020 delivered in Abeokuta, Ogun State on the 9th day of December 2020 by Hon. Justice Ibrahim Watila (of blessed memory).
826 In Federal Ministry of Health v Trade Union Members of the Joint Health Sector Union (2014) LPELR–23546 (CA), it was defined as 'without loss of any rights in a way that does not cancel the legal rights of any party' while in Nawa v Attorney General, Cross River State (2008) All FWLR (Pt. 407) 807, it was defined as 'without affecting any other legal matter.' See also Umeji v Attorney General of Imo State (1995) 4 NWLR (Pt. 391) 55.
827 Johanna Chamberlain and Jane Reichel, 'The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation (2020) 89 Mississippi Law Journal, 1; Eton O'Dell, 'Compensation for Breach of the General Data Protection Regulation' (2017) 40(1) Dublin University Law Journal, 97–164.

with ARP lack the power to award damages to violation of data protection rights.

CHAPTER NINETEEN

Administrative fines and damages

Data protection laws principally set rules for the protection of personal information through the regulation of processing operation by business with sanctions in the event of default. Applicable penalties for violation of data protection principle and/or data subjects' rights varies from administrative fines, corrective directives, damages or even imprisonment.[828]

National DPAs are usually equipped with powers to impose administrative fines[829] on data controllers generally for the violation of data protection laws but this does not necessarily translate into remedies for data breach suffered by data subjects.[830]

Under, the NDPR, curiously data controllers are penalized with fine for breach of data subjects' rights as opposed to breach of the entire regulation itself.[831] The NDPR, unlike the GDPR and English Data Protection Act which expressly provide for 'administrative fines' simply imposes 'fines' on controllers and this blanket use of the word 'fines' is problematic when the decisions of the Nigerian courts on the concept of 'fine' are considered. In *Bashir v Federal*

828 Some African data protection laws have provision on imprisonment, see articles 51–60 of the Angolan Law No. 22/11 on data protection; Burkina Faso's Law No. 010–2004/AN provides between three to five years for data breach; Tunisia Organic Act No. 2004–63 stipulates five years imprisonment etc.
829 GDPR, art.83, UK Data Protection Act, 2018, s.196.
830 The GDPR however makes separate provision for compensation although same rules may be applicable to both fines and damages. See GDPR, art. 83 and UK Data Protection Act, 2018, s.196.
831 By reg. 2.10 NDPR, controllers are liable to be fined for the tune of N10, 000, 000 (Ten million Naira) or 20% of annual gross revenue for breach of data privacy rights.

Republic of Nigeria[832] the Court of Appeal defined the term as a 'pecuniary penalty imposed by a competent court upon a person convicted of a crime.' Earlier, the same court in *Surajo Abdullahi v Kano State*[833] described the term elaborately as 'strictly restricted to crimes' and as 'a payment of money ordered by a court from a person who has been found guilty of violating law. It may be specified as the punishment for an offence, usually a minor offence but could also be specified and used as an option to imprisonment for major crime or a complement to other punishments specified for such crimes.' [834] Having defined the term, the Court of Appeal went ahead to categorically emphasize in the case of *National Oil Spill Detection and Response Agency (NOSDRA) v Mobil Producing Nigeria Unlimited* that: 'it is very well known in law that a fine is a criminal sanction.... I might underline the fact that awarding a fine is a judicial act and it is the sole prerogative of a court of law... no other organization or bodies can usurp that power. Any law that would consign to anybody other than the courts power to award fine is unconstitutional.'[835]

However, the same Court of Appeal had earlier in *Corporate Affairs Commission v Seven Up Bottling Company*[836] ruled that, a public body can issue fines without necessarily going through the courts or criminal prosecution procedure.[837] Lateef and Taiwo conclude that, although fines issued within the context of NITDA Act (pursuant to which the NDPR was purportedly issued) is ultra vires, the absence of any judicial decision to the contrary makes it permissible in the circumstance.[838] It is however worthy of note that, the High Court of Ogun State ruled in the case between

832 (2016) LPELR–40252 (CA).
833 (2015) LPELR–25928(CA).
834 (2015) LPELR–25928(CA).
835 (2018) 13 NWLR (Pt. 1636) 334.
836 (2017) 5 NWLR (Pt. 1558) 241.
837 See also Moses Edrisu v Federal Road Safety Commission (2016) 4 NWLR (Pt. 1502) 209; Ebong v Securities and Exchange Commission (2017) LPELR–43547 (CA).
838 M.A. Lateef and I.O. Taiwo, 'Examination of the Legal Regime for Information Privacy, Data Protection and Enforcement of Sanctions in Nigeria' (2020) 3 Elizade University Law Journal, 151, 184.

Incorporated Trustees of Digital Rights Lawyers Initiative and LT Solutions & Multimedia Limited[839] that, imposition of fine under the NDPR is a criminal or quasi criminal issue but the court did not rule on NITDA's competence to issue such fines.

Notwithstanding the desirability of administrative fines as a tool for strengthening enforcement of data protection legislation in Nigeria, the rules governing issuance of such fines are universally subject to respective country's municipal laws regulating the procedure and competent bodies.[840] From the foregoing decisions, the current position of Nigeria law is such that, fines can only be issued by national courts until the subsisting decision in NOSDRA[841] is upturned by the Supreme Court.

Damages

A universal principle regulating breach of fundamental right is– Ubi jus ibi remedium–meaning, where a right has been violated, remedy must automatically accrue. In *Iwununne v Egbadiem*,[842] the Court of Appeal noted that, in fundamental rights matters, damages automatically accrue, once there is a breach of violation of rights.[843] However, often times, victims of data breach may not suffer pecuniary loss but since it is a violation of rights, one need not prove material damages, as compensation can be awarded for distress and generally for commission of wrong by a controller,[844] more so, the NDPR also contemplates remedies in the event of

839 (Unreported) Suit No. HCT/262/2020 delivered by Ogunfowora, J. on Monday, 9th day of November 2020 in Abeokuta, Ogun State.

840 For example, under the GDPR, it is acknowledged that the Danish and Estonian legal systems do not allow blanket issuance of administration fines by the DPAs. While only courts can impose fines as criminal penalty in Denmark, the DPA issues fine in a misdemeanour (criminal) procedure.

841 The decision in NOSDRA's case is the most recent of all the conflicting decisions on this issue and by the doctrine of stare decisis, it remains the position of the law until set aside. See Fabunmi v University of Ibadan (2016) LPELR–41132(CA), Comptroller General of Prisons v Idehen (2009) LPELR–4003 (CA).

842 (2016) LPELR–405159 (CA).

843 See also Ozide v Ewuzie (2015) LPELR–24482 (CA), Okoro v Commissioner of Police, Enugu state (2016) LPELR–41025(CA) and Okonkwo v Ogbogu (1996) 5 NWLR (Pt. 499) 420.

844 See Shobna Gulati v MGN Limited (2015) EWHC 1482 (Ch).

violation of data subjects' rights.[845]

845 NDPR, reg.2.5(g)(h) and 4.2(1).

CHAPTER TWENTY

International transfers of data

DATA PROTECTION IS a global issue that necessitates universal and regional frameworks for seamless cooperation between the national DPAs to properly monitor and protect the international transfer of data within their borders.[846] The European Convention 108[847] is reputed to have made the first legislative reference to cooperation between national DPAs for the enforcement of cross border transfer of personal data within Council of Europe (CoE) member states by setting up a robust system for reciprocal support within the region.[848] The OECD Guidelines of 1980 however dealt with international data transfer but they are not a binding instrument and later in 2007, the OECD[849] issued further recommendations on cross border cooperation.[850]

In Europe, in the event of transborder data breach, the GDPR encourages some level of cooperation among the national DPAs concerned to ensure uniformity in investigation and decision

846 Charles D. Raab, 'The Governance of Global Issue: Protecting Privacy in personal information in New Modes of Governance in the Global System International Policy Economy Serves (Palgrave Macmillan London 2006
847 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is a 1981 treaty of the Council of Europe ratified by all members of the council and non–members like Argentina, Cape Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay.
848 See Graham Greenleaf, 'How Far Can Convention 108 Globalise? Prospects for Asian Accessions' (2020) Computer Law & Security Review, 3.
849 Organisation for Economic Co–operation and Development.
850 Christopher Kuner, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past Present and Future' (2011) OECD Digital Economy Papers No 187, OECD Publishing.

making[851] and for this purpose, the European Commission maintains a list of competent national DPAs and contact points to facilitate some measure of consistency in their approach to data breaches.[852]

In forging an alliance to facilitate international transfer of data, eleven DPAs formed the Global Privacy Enforcement Network (GPEN) in March 2010 for the purpose of 'connecting privacy enforcement authorities around the world to promote and support cooperation in cross border enforcement of laws protecting privacy but this action plan does not create a binding obligation.[853]Under the repealed EU Data Protection Directive 95, national DPAs were duty bound to cooperate with one another in the performance of their duties[854] but over time, countries and their DPAs have also come to the realization of the essentiality of co–regulation of transborder transfers of personal data.[855]

In Nigeria, NITDA is mandated by the NDPR to 'develop' international cooperation mechanisms and 'provide mutual assistance' to facilitate the effective enforcement of legislation for the protection of personal data.[856] Unfortunately, Nigeria has neither ratified the Malabo Convention nor domesticated the ECOWAS Supplementary Act on data protection which international instruments require member states to adopt legislative measure for regional cooperation and to ensure mutual assistance[857] while in its preamble, the ECOWAS Supplementary

851 Apostolos Malatras, Ignacio Sanchez, Laurent Beslay, Iwen Coisel, Loannis Vakalis, Giussepe D'Acquisto, Manuel Sanchez, Matthieu Grall, Marit Hansen and Vasilios Zorkadis, 'Pan European Data Breaches: Mapping of Current Practices and Recommendation to Facilitate Cooperation Among Data Protection Authorities' (2017) 33 Computer Law & Security Review, 458–469.
852 GDPR, art. 2(5).
853 In the same vein, an annual gathering of national DPAs also shape policies around data transfer across borders during the international Conference of Data Protection and Privacy Commissioners (ICDPPC).
854 Article 28(6).
855 Dariusz Kloza and Anne Moscibroda 'Making the case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insight from Corruption Law' (2014) 4(2) International Data Privacy Law, 120.
856 NDPR, reg. 4.3(a) and (b).
857 African Union Convention on Cyber Security and Personal Data Protection, art. 28. (1), (2) and (3).

Act specifically alludes to a harmonised legal framework for data protection.[858] It is however arguably that the ECOWAS Supplementary Act is immediately enforceable in Nigeria by virtue of article 48 which makes the treaty an integral part of the ECOWAS Act that has already been domesticated in Nigeria.[859]

Despite the non–existent binding international legal framework guiding NITDA's regulation of cross border transfers, especially in relation to its cooperation with some other African national DPAs, its membership of the African Network of Data Protection Authorities, Common Thread Network (CTN), and African Network of Data Protection Authorities arguably aids its social cooperation with other national NDAs.[860]

858 Alex B. Makulilo, 'Myth and Reality of Harmonization of Data Privacy in Africa' (2015) 31(1) Computer Law & Security Review, 78–89.
859 Helen Chuma–Okoro, 'The Nigerian Constitution, the ECOWAS Treaty and the Judiciary: Interplay of Roles in the Constitutionalisation of Free Trade' (2020) 4(1) Global Journal of Comparative Law, 43.
860 CTN is a forum of national supervising authority focusing on cross border mutual assistance etc.) see h<ttps://www.commonthreadnetwork.org/#:~:text=The%20Common%20Thread%20Network%20(CTN)%20is%20a%20forum%20for%20data,practices%20for%20effective%20data%20protection.> accessed 6 May 2021; <https://www.rapdp.org/en> accessed 10 May 2021. RADPA is a Pan African dialogue of National DPAs in the continent. https://id4africa.com/2019–radpa/> accessed 6 May 2021.

CHAPTER TWENTY–ONE

Personal Data Breach

A PERSONAL DATA BREACH is a deliberate or accidental disclosure or exposure of personal data to unauthorized persons or bodies.[861] It is the 'unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data'[862] and could also be 'a security incident either intentional or unintentional, where unauthorized entities gain the control of personal data or otherwise protected or confidential data.'[863]

Personal data breach has been regulatorily defined to mean the 'breach of security leading to accidental or unlawful destination, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted or stored or otherwise processed.'[864] The foregoing definition however reveals that, not all types of security breaches qualify as data breach especially in cases where they do not lead to the events listed therein. In other words, some security breaches may merely qualify as security incidents but not personal data breach.[865]

861 Long Cheng, Fang Liu and Danfeng Yao, 'Enterprise Data Breach: Causes Challenges, Prevention and Future Directions' (2017) < https://onlinelibrary.wiley.com/doi/full/10.1002/widm.1211>accessed 20 June 2021.
862 Ravi Sen & Sharad Borle, 'Estimating the Contextual Risk of Data Breach: An Empirical Approach' (2015) 32(2) Journal of Management Information Systems, 314–341.
863 See Dimitris Geneiatakis & Stefan Scheer, 'Personal Data Breaches' (2013) Joint Research Centre, European Commission, 7.
864 GDPR, art 4(12). This definition is also adopted by the NDPR, reg. 1.3(xxii).
865 Data security incident is an unintended event indicating that the controller's data protection system has been compromised but falls short of unauthorized exposure to third parties.

For an event to qualify as personal data breach under most data protection legislation, it must (a) interfere with data security measure(s); and (b) must lead to accidental or unlawful destruction or loss or alteration or modification or storage or theft or any other unauthorised dealing with personal data. It thus follows that, where personal data is transmitted without a security breach, it may not constitute personal data breach.

Personal data breaches can occur through cyberattacks, accidental sending of emails to unintended recipients, loss or destruction of device storing personal data, breaking into offices where personal data are kept, disgruntled staff stealing personal data for untoward use.[866]

Data controller's obligation

In the event of personal data breaches, data controllers are obliged to inform the DPA or data subjects of the nature of the breach in certain cases as delineated by relevant laws.[867] The NDPR does not make provisions for data breach notification but its Implementation Framework[868] requires data controllers to notify NITDA with 72 hours of the breach by disclosing: (a) a description of the data breach; (b) the date or time period of breach; (c) a description of the personal data breached; (d) an assessment of the risk posed by the breach; (e) an estimate of the number of data subjects likely affected; (f) a description of steps the organization has taken to reduce the risk of harm to individuals; (g) a description of notification steps taken by the controller, and (h) the name and contact information of an employee of the controller who can answer regulator's questions about the data

866 See the case of WM Morrison Supermarkets Plc v Various Claimants (2020) UKSC 1.
867 Maria Karyda and Lilian Mitrou, 'Data Breach. Notification issues and Challenges for Security Management' (2016) Tenth Mediterranean Conference on Information System (MCIS) Paphos, Cyprus, September 2016.
868 NDPR Implementation Framework was issued in November 2020 by NITDA found at < https://nitda.gov.ng/wp–content/uploads/2021/01/NDPR–Implementation–Framework.pdf> accessed 1 July 2021.

breach.[869]

Where the incident or breach is, in the reasonable opinion of the controller, not likely to result in a risk to the rights and freedoms of data subjects, then notification is neither required to the DPA nor the data subjects. It must however be stated that, this is quite tricky because, the parameters for measuring such risks remain unclear even under the more developed European jurisdiction.

Data processor's obligation

In Europe, since processors are contractually engaged to process data on behalf of controllers, while they do not have obligation to notify the DPA of data breach, but they are duty–bound to inform their 'principals' without undue delay once they become aware of such data breach. Conversely under the NDPR, data processors share same duty of notification with the controllers, hence once they become aware of data breach, they must notify NITDA within 72 hours.[870] This notification requirement under the Implementation framework is however misplaced since processors are recruited by controllers, it ought to be the exclusive duty of the latter to determine when an incident constitutes a breach enough to trigger the notification requirement.

Types of personal data breach

Personal data breach could occur in many forms with varying consequences or effects[871] on the data subjects as dictated by the reason(s) for the breach and/or motive of the invader (if any).

869 NDPR Implementation Framework, clause 9.3(a) –(h).
870 NDPR Implementation Framework, clause 3.2(ix).
871 Identity theft is one of the end products of personal data breach if not adequately and timely managed. See Fabio Bisogni and Hadi Asghari, 'More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws' (2020) 10 Journal of Information Policy, 45–82.

Confidentiality breach occurs where personal data is disclosed without the consent or authority of the data subject or a third–party gains access to such information without the former's consent. This type of breach is common in privileged relations e.g between Solicitor and Client or situations concerning health and medical records where a patient's health status is disclosed to a third party without such patient's consent or authorisation.

Integrity breach is the alteration or modification of personal data without the data subject's knowledge, consent or authorisation thereby compromising data quality. This breach could be committed by a controller or a third party or hacker who comes in contact with personal data, alters it to suit his ulterior purpose before transmitting same to the intended recipient.[872]

Availability breach is committed when access of personal data is prevented from the authorised person(s). This breach may be temporary or permanent and could be occasioned by non–malicious causes especially in the event of system downtime or network failure preventing momentary access to personal data. It could result in total loss or destruction of data or lack of access to same.

Utility breach is the unauthorised use of personal data by controllers or third parties without data subject's consent. Here, although personal data is collected with data subject's consent, such data is misused for unintended purposes.

Possession breach occurs when a party stores and retains a data subject's personal data without his knowledge or consent.

872 This is sometimes referred to as 'accuracy breach.'

CHAPTER TWENTY–TWO

Suggested Reforms

Privacy has been part of Nigeria's constitutional framework since the mid–fifties[873] but the fundamental right has neither enjoyed the desired academic attention nor sufficient judicial pronouncements. Data protection on the other hand effectively became a national concern in 2019, even though sectoral legislation had relevant provisions on the subject prior to the issuance of the NDPR, not so much had been done in terms of enforcement or capacity building. This chapter briefly discusses some necessary reforms for the Nigerian data protection ecosystem.

a. Principal legislation on data protection

Out of the 54 countries in Africa, 29 have principal data protection legislation but only Nigeria has a subsidiary legislation[874] which was purportedly issued pursuant to provisions of a law which do not expressly confer such powers on the self–assigned regulator. The NDPR has been repeatedly criticised to be inadequate, contradictory, and ultimately lacking the force of law enjoyed by principal legislation. It was described as a 'stop gap' by the World bank[875] and this much was admitted when the Federal

873 Pre–independence Nigeria (Constitution) Order in Council 154 (Lyttleton Constitution) provided for right to privacy in its schedule.

874 Graham Greenleaf and Bertil Cottier, 'Comparing African Data Privacy Laws: International, African and Regional Commitments' (2020) University of New South Wales Law Research Series, 32.

875 The World Bank, 'Nigeria Digital Economy Diagnostic Report' (2019) <http://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria–Digital–Economy–Diagnostic–Report.pdf> accessed 17 May 2021.

Government, through NITDA invited comments from the public on a draft Data Protection Bill in August 2020.[876]

The enactment of a principal data protection Act by the Nigerian Government is long overdue given the long list of its failed legislative attempts in the past and it is hoped that, such law will set the tone for a comprehensive legal system for data protection in the country.

b. Independent data protection authority (DPA)

NITDA currently acts as Nigeria's DPA but it does not only lack statutory legitimacy to so act, it is plagued by many inhibitions in the performance of its self–imposed functions as Nigeria's DPA. The agency's board is solely appointed by the President who does not only hold the power to fire the members at will, but the enabling Act also subjects the agency's chief executive to the directive of a cabinet minister[877] on the exercise of his functions.

The agency's perceived unhealthy relationship with the government has hindered its unbiased and impartial performance of duty, contrary to the provisions of ECOWAS Supplementary Act which requires membership of such bodies to be incompatible with civil service to ensure some level of independence and impartiality. [878]

A robust data protection legal framework starts and ends with an independent, skilful, knowledgeable, and professional DPA, hence Nigeria needs to set up an independent and wholly dedicated regulator for her data protection ecosystem as soon as practicable.

876 One Trust Data Guidance, 'Nigeria: NITDA publishes draft Data Protection Bill 2020 for public comments' (2020)https://www.dataguidance.com/news/nigeria–nitda–publishes–draft–data–protection–bill–2020–public–comments accessed 1 June 2021.
877 NITDA Act 2007, section 31.
878 ECOWAS Supplementary Act on personal data protection, art. 16.

c. Administrative redress mechanism.

Most data protection laws in the world are embedded with provisions establishing some administrative redress mechanism which internally addresses allegations of breach of data subjects' rights and provide appropriate reprieve to victims. The NDPR contemplates an Administrative Redress Panel (ARP) but it was never constituted, hence data subjects are left with no remedies except they approach the courts. The importance of an internal administrative redress body cannot be over emphasized especially in Nigeria where the cost of justice delivery is rather high in terms of financial resources and time consideration. It is advisable for the government to timely set up an internal redress panel to adequately resolve data breach complaints which are on the rise in the country.

d. Academic intervention

Prior to the publication of this book, Nigeria had no single textbook on privacy. The country's first law (case)book on data protection was published in June 2020[879] and it 1s predominantly based on foreign materials without referencing any publication on Nigerian law. The NDPR is over two years, yet, data protection law and practice in Nigeria have not received sufficient academic attention deserving of such a global subject. The field is devoid of many research and academic writings; hence its growth has been stunted within and outside the classrooms. The University curriculum in Nigeria needs to be reviewed to include data protection as one of the courses and this will not only bridge the knowledge gap from the University level, but it will also increase the quantum of research work undertaken in the field.

879 Olumide Babalola, *Casebook on Data Protection,* (ISBN: 978–620–2–55355–1) Noetico Repertum, 2020).

e. Certainty of case law

The development of any area of law largely depends on judicial disposition towards same. With respect to data protection, the Nigerian judiciary needs to take a firm position on whether or not the concept would be approached as a fundamental right or another normative concept with less sanctity. There exist conflicting decisions as to whether data protection is contemplated under the constitutionally guaranteed right to privacy or whether it is another right created by other legislation.[880] This conflict must be permanently resolved one way or the other by the courts before the concept can fully thrive in Nigeria as far as its enjoyment and enforcement are concerned.

880 Olumide Babalola, 'Privacy Versus Data Protection Debate in Nigeria: The Two Schools of Thought' (2021) < https://www.researchgate.net/publication/349879979_Privacy_Versus_Data_Protection_Debate_in_Nigeria_The_Two_Schools_of_Thought> 1 July 2021.

Bibliography

Abdulrauf, A, L and Fombad, M, C, 'Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms' (2016) 38(2) Liverpool Law Review,

Abdulrauf, A, S 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' published LLD thesis, University of Pretoria, 2015.

Acquisti, A, Privacy and Rationality in Individual Decision–Making IEEE Security Privacy 3(1) 26.

Adepetun, A 'Why Buhari Should Assent to the Data Protection Bill' https://guardian.ng/technology/why–buhari–should–assent–to–data–protection–bill/ accessed 16 March 2021.

African Union Convention on Cyber Security and Personal Data Protection, art. 28. (1), (2) and (3).

Agbozo, E, Alhassan, D and Spassour, K 'Personal Data Privacy Barriers to E–Government Adoption, Implementation and Development in sub–Saharan Africa' in Electronic Governance and Open Society: Challenges in Eurasia (Springer International, 2018).

Agiri, B, The Concept and Practice of Individual Rights in Nigeria 1950–1966: How Relevant is the American Constitutional Experience (1991) 29(2) American Studies International 55–68.

Ajayi, G 'African Response to the Information Communication Technology Revolution: Case study of the ICT Development in Nigeria' African Technology Policies Study (ATPS) Special Paper 8, African Technology Policy Network, Nairobi, Kenya.

Akanji, J, O, and Adeleke, S, B 'Subscribers Attitude Towards Unsolicited Text Messages (UTM) Among Nigerian Telecommunication Firms' (2018) 3(3) European Journal of Management and Marketing Studies, 3

Akpan, E, M 'The 1979 Nigerian Constitution and Human Rights' (1980) 2(2) Universal Human Rights, 23.

Akpan–bong, I, P Information and Communication Technologies in Nigeria: Prospects and Challenges for Development (Peter Lang Publishing, 2009) 203.

Aldrich, F, 'Smart Homes' Past, Present and Future' in Inside Smart Homes Richard Harper (ed) (Springer 2008).

Alex B. Makulilo, African Data Privacy Laws (Springer, 2016)

Al–Fedaghi, S, 'The Right to be let Alone' and Private Information' In: Enterprise Information Systems VII, Chin–Sheng Chen, Joaquim Filipe, Isabel Seruca and José Cordeiro, (eds) Springer, 2007).

Ali, B, and Awad, A, I 'Cyber and Homes (2018) 18(3) Sensors (Based) 817

Alitajer, S, & Nejoumi, M, G, Privacy at home; Analysis of Behavioural Patterns in the Spartial Configuration of Traditional and Modern Houses in the City of Hamedan Based on the Notion of Space Syntax (2016) 5 frontiers of Architectural Research 341–352)

Aliyu, S, A, 'The Nigerian Data Protection Bill: Appraisal, Issues and Challenges'

Alkali, U, A, Jimeta, A, Magashi, I, A, and Buba, M, T 'Nature and Sources of Nigerian Legal System: An Exorcism of a Wrong Notion' (2014) 5(4) International Journal of Business, Economics and Law, 1.

Allen, A, Associational Privacy and the First Amendment: NAACP v Alabama, Privacy and Data Protection (2011) 1 Alabama Civil Rights & Coral Liberties Law Review ,13.

Allen, A, Privacy Torts: Unreliable Remedies for LGBT Plaintiffs (2010) 98 California Law Review 1711–1721);

Allen, A, Race, Face and Rawls (2004) 72 Fordham Law Review, 1677–1696.

Allen, A, Taking Liberties: Privacy, Private Choice and social Contract Theory (1998) 56 UC in L Rev 411, 466.

Allen, A, Unpopular Privacy: What We Must Hide (Oxford University Press, 2011) 259.

Alsenoy, A, J V, B and Dumortier, J 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions in Managing Privacy Through Accountability, Daniel

Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener & Hector Postigo (eds) (Palgrave and Macmillan, 2012) 27.

Alsenoy, B, Kindt, E and Dumortier, J 'Privacy and Data Protection Aspects of e–Government Identity Management' in Innovating Government, Simone van der Hof, Marga M. Groothuis (eds) (Springer, 2011).

Altman, I, The Environment and Social Behavior, Privacy, Personal Space, Territory and Crowding (Monterey Books, 1975) 1.

Aluko, O, and Kodilinye, G, The Nigerian Law of Torts (Spectrum Books, Ibadan, 2001).

Amine, H and Mesnaoui, A 'Electronic Data Interchange (EDI) in the Supply Chain: Impact on Customer Satisfaction' (2018) 4(6) Journal of Business Management, 15.

Aminifar, A, Ka Pun, V, L, Yand Rabbi, F 'A Practical Methodology for Anonymization of Structural Health Data' (2019) SHI 2019. Proceedings of the 17th Scandinavian Conference on Health Informatic Informatics, Oslo, Norway, 1.

Anderson, T, 'Balancing the Scales: Re–Instating Home Privacy Without Violence In Indiana' (2013) 88(1) Indiana Law Journal 391.

Andres Calderon, Susana Gonzales and Alejandra Ruiz, 'Privacy, Personal Data Protection and Freedom of Expression Under Quarantine? The Peruvian Experience' (2021) 00(0) International Data Privacy Law, 11.

Anne de Hingh, 'Some Reflections on Dignity as an Alternative

Legal Concept in Data Protection Regulation' (2018) 19(5) German Law Journal, 1270.

Anozie, C, M, Abortion and Homosexuality Prohibitors Regimes Versus the Right to Privacy in Nigeria' (2020) 46 (3) Commonwealth Law Bulletin 483, 486.

Antoniadis et al, J Separating the Roles of CEO and Chairman of the Board. The Case of Greek Listed Firms in Accounting and Finance in Transition (vol. 11 Greenwich University Press, 2005).

Antoon De Baets, 'The Impact of the Universal Declaration of Human Rights on the Study of History' (2004) 48(1) History and Theory, 20–43.

Arkenhead, M, A Reasonable Expectation of Sexual Privacy in Digital Age (2018) 41 Dalhousie L.J 273.

Auloos, J, Mahieu, R & Veale, M 'Getting Data Subjects Rights Right. A Submission to the European Data Protection Board from International Data Rights Academics to Inform Regulatory Compliance' (2021) 10 JIPITEC, 1.

Ausloos, J, Mahieu, R and Veale M 'Getting Data Subjects Rights Right. A Submission to the

Babalola, O 'A Bird's Eye Rundown on Nigeria's Data Protection Legal and Institutional Model' (2021) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3808570> accessed 13 May 2021.

Babalola, O Babalola's Law Dictionary of Judicially Defined Words and Phrases (2nd edn, Noetico Repertum, Lagos, 2019) 352.

Babalola, O *Casebook on Data Protection* (Noetico Repertum, Lagos, 2020) 230.

Babalola, O, Privacy Versus Data Protection Debate in Nigeria: The Two Schools of Thought (2021)

Babalola, O, 'A Bird's Eye Rundown on Nigeria's Data Protection Legal and Institutional Model' (2021) 12(2) Gravitas Review of Business & Property Law, 1.

Babalola, O, 'Does the Nigerian Constitution expressly provide for a 'right to private and family life'?: Re–interrogating the effect of the marginal note in section 37 of the Constitution of the Federal Republic of Nigeria 1999' https://esq–law.com/does–the–nigerian–constitution–expressly–provide–for–a–right–to–private–and–family–life.html accessed 13 April 2021.

Babalola, O, 'The Statutory Tort of Invasion of Privacy Under the Law Reform (Torts) Law of Lagos State. Ch. L82 of 2015 and the Recent Spate of Data Breaches in Lagos State' (2020) < https://www.mondaq.com/nigeria/privacy–protection/892014/the–statutory–tort–of–invasion–of–privacy–under–the–law–reform–torts–law–of–lagos–state–ch–l82–of–2015–and–the–recent–spate–of–data–breaches–in–lagos–state#:~:text=L82%20Laws%20of%20Lagos%20State,offensive%20to%20a%20reasonable%20person.> accused 29 March 2021.

Babalola, O, Babalola's Law Dictionary (2nd ed. Noetico Repeturm Lagos ,2019) 346

Bailey, D, K, Typologies and Taxonomies: An introduction to Classification Techniques (Sage Publication, California, 1994) 6.

Bainbridge, D and Pearce, G 'Tilting at Windmills–Has the New Data Protection Law Failed to Make a Significant Contributions to Right to Privacy' (2000) Journal of Information, Law and Technology, 2.

Banerjee, A, Nordquist, M, and Hellerstedt, K, 'The Role of the Board Chair–A Literature Review and Suggestion for Future Research' (2020) 28 Corporate Governance International Review, 372–405.

Banisar, B, Privacy and Data Protection Around the World (1999) Conference Proceedings of 21st International Conference on Privacy and Personal Data Protection Hong Kong

Bannerman, Relational Privacy and the Networked Governance of the Self? (2019) 22(14) Information, Communication and Society 2187–2202.

Bannister, F and Connolly, R 'Defining E–Governance' (2012)8(2) E–Service Journal, 3–25.

Barka, M, 'Data Protection and Conflict of Laws: A Challenging Relationship' (2016) 2(3) European Data Protection Law Review, 324–341.

Bart van der Sloot 'Decisional Privacy 2.0: The Procedural Requirements Implicit in Article 8 ECHR and its Patents Impact on Profiling' (2017) 7(3) IDPL 190–201.

Basheer A.M. Al–lak. And Ibrahim A.M. Alnawasi, 'Mobile Marketing: Examining the Impact of Trust, Privacy Concern and Consumer's Attitude on Intention to Purchase' (2010) 5(3) International Journal of Business and Management, 29.

Belanger, F, and Crossler, R, Privacy in Digital Age: A Review of Information Privacy Research in Information Systems' (2011) 35(4) MISQ. 1017–1041.

Belanger, F, Hiller, S, J, and Smith, J, Trustworthiness in Electronic Commerce; The Role of Privacy, Security and Site Attributes (2002) 11 Journal of Strategic Information Systems, 245–270.

Benett, J, C 'The Accountability Approach to Privacy and Data Protection: Assumptions and Cavaets' in Managing Privacy Through Accountability, Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener & Hector Postigo (eds) (Palgrave and Macmillan, 2012) 27.

Benjami Bratman, 'Brandeis and Warren' The Right to Privacy and Birth of the Right to Privacy (2002) 69 Tenn. Law Review 623.

Bennet, CJ, The Privacy Advocates: Resisting the Spread of Surveillance (Massachusetts Institute of Technology, 2008) 76.

Bennet, J, C 'International Privacy Standards: Can Accountability be Adequate? (2010) 106 Laws and Business International, 3.

Bennet, J, C, Regulating privacy, Data Protection and Public Policy in Europe and United States (Cornel University Press, 1992) 288.

Bergemann, B 'The Consent Paradox: Accounting for the Prominent Role of Consent' in Data Protection (2018) in Privacy Identity Management. The Smart Revolution, Hansen, M, Nai–Formo, E, I, Habner, F, S (eds) (Springer International Publishing, 2018) 111–131.

Bertino, E 'Data Security: Challenges and Research Opportunities' (2013) Secure Data Management, 9–13.

Best, D, Mind, Act and Philosophy (1986) 20(3) The Journal of Aesthetic Education, 16, 17.

Beswick, S, and Fother, W, by, 'The Divergent paths of Commonwealth Privacy Torts' (2018)84(2d) Supreme Court Law Review, 225–267

Bevier, L, Information about Individuals in the Hands of Government: Some Reflections on Mechanism for Privacy Protection (Won Mary & Bill Rt. 1995) 455.

Biega, J, A, Potash, P, Daume, H, Diaz, F, and Fink, M, 'Operationalizing the Legal Principle of Data Minimization for Personalization' (2020) SIGIR, Virtual Event, China, 399, 400.

Blackstone, W, Commentaries on laws of England (1769).

Blokdyk, G, Data Privacy. A Complete Guide (Create Space Independent Publishing Platform, 2018)

Blume, P, 'Data Protection and Privacy–Basic Concepts in a Changing World' (2010) Scandinavian Studies in Law, 151.

Blume, P, Data Protection and Privacy–Basic Concepts in a Changing World (2010) Scandinavian Studies In Law, 151.

Bodwell, W & Chermack, T 'Organizational Ambidexterity: Integrating Deliberate Emergent Strategy with Scenario Planning, Technological Forecasting and Social Change, 77.

Bok, S, Secrets on Ethics of Concealment and Revelation (Phantom books, New York, 1983).

Borgesius, Z, 'Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis, University of Amsterdam, 2014).

Borghi, M 'Data Portability and Regulation of Digital Markets' (2019) Centre for Intellectual Property Policy & Management, Working Papers No. 02–2019, 3.

Bork, R, The Tempting of America: The Political Seduction of the Law, Free Press, New York, 1990)

Brasher, E 'Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation' (2018)1 Columbia Business Law Review, 209–253.

Brooks, G Data Protection; Tougher Penalties for Data Protection Offenses (2007) 9(1) Journal of Direct, Data and Digital Marketing Practice, 86.

Brown, G, The Universal Declaration of Human Rights in the 21st Century: A Living

Buckle, P 'Data subject Access Request and Beneficiaries' Right to Information' (2019)'25(3) Trusts and Trustees, 328–342.

Bufaleiri, L, Morgia, M, Mei, A & Stufa, J 'GDPR: When the Rights to Access Personal Data Becomes a Threat' (2020) IEEE, 1.

Bugeja, J, Jacobsson, A and Davidsson, P, 'On Privacy and Security Challenges in Smart Connected Homes (2016) European

Intelligence Security Informatics Conference.

Buitelaar, C, J, Post–Mortem Privacy and Informational Self–Determination (2017) 19 Ethics Information Technology, 129–162.

Burleson, D 'A Comprehensive Definition of Electronic Data'

By reg. 2.10 of the NDPR, controllers are liable to be fined for the tune of N10,000,000 (Ten million Naira) or 20% of annual gross revenue.

Bygrave, A,L Data Protection Law: An International Perspective (Oxford University Press, 2014)

Bygrave, A,L Data Protection Law; Approaching its Rational, Logic and Limits (Kluwer Law International, 2002) 2).

Bygrave, A,L, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology, 247.

Bygrave, A,L, 'European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation' (2000) 16(4) Computer Law & Security Review, 252–257.

Bygrave, A,L, Privacy Protection in a Global Context–A Comparative Overview (2004) 47 Scandinavian Studies in Law 319–348 at p. 328

Bygrave, A,L, 'The Place of Privacy in Data Protection Law' (2001) University of New South Wales Law Journal 241, 277–283.

Calista, J, D and Melitski, J "E–Government And E–Governance:

Converging Constructs of Public Sector Information and Communications Technologies' (2007) 31(1) Public Administration Quarterly, 87–120

Cambridge Advance Learner's Dictionary (3rd edn, Cambridge University Press, 1995)

Carlson, S Executive Behaviour. A study and the Working Method of Managing Directors. (Stockhlom, Stromberg, 1951).

Carolan, F, The Concept of a Right to Privacy' in The Right to Privacy: A Doctrinal and Comparative Analysis Hillary Delancy and Eoin Carolan. (eds) (Round Hall, 2008).

Carvalho et al, M, R 'Protecting Citizens' Personal Data and Privacy Joint Effort from GDPR EU Cluster Research Projects' (2020)1(217) SN COMPUT. SCI, 1,13.

Casey, B, Farhangi, A, and Vogl, R, 'Rethinking Explainable Machines: The GDPR's Right to Explanation' Debate and the Rise of Algorithm Audits in Enterprise' (2019) 34(1) Berkeley Technology Law Journal, 143–188.

Cate, H, F 'The Failure of Fair Information Practice Principles' in Consumer Protection in the Consumer Protection in the Age of Information Economy, Jane K. Winn (ed) (Ashgate, 2006) 341.

Chamberlain, J and Reichel, J 'The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation (2020) 89 Mississippi Law Journal, 1;

Chamberlain, J and Reichel, J 'The Relationship Between Damages and Administrative Fine in the EU General Data Protection

Regulation' (2020) 89(4) Mississippi Law Journal, 668, 691.

Chapman, I, J 'Local Government, Fiscal Autonomy and Fiscal Stress: The Case of California' (1999) Lincoln Institute of Land Working Paper.

Chen, J, 'The Dangers of Accuracy: Exploring the other side of the Data Quality Principle' (2018) 4 European Data Protection Law Review, 36, 37–81.

Chen, J, Edwards, L, Urguhart, L and McAuley, D 'Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020)10(4) International Data Privacy Law, 279, 280.

Chen, Y–C and Hseish, J–Y 'Advancing E–Government: Comparing Taiwan and the United States' (2009) 69 Public Administration Review, 151–158.

Cheng, L, Liu, F and Yao, D 'Enterprise Data Breach: Causes Challenges, Prevention and Future Directions' (2017) <https://onlinelibrary.wiley.com/doi/full/10.1002/widm.1211>accessed 20 June 2021.

Chijioke,C, Crime and Criminal Investigation in Nigeria; A study of Police Criminal Investigations in Enugu State (2013) 1 International Journal of Africa and Asian Studies.

Chika, D, and Tochukwu, E, 'An Analysis of Data Protection and Compliance in Nigeria' (2020) 4(5) International Journal of Research and Innovation in Social Science (IJRISS) 377,

Chinyere, C, A, 'Rudiments of Human Rights' (2016) 1(2010)

Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 1.

Chitayat, G 'Working Relationships Between Chairman of the Board of Directors and the CEOs' (1984) 24 Management International Review, 65–70

Christopher Docksey, 'Four Fundamental Rights: Funding the Balance' (2016) 6(3) International Data Privacy Law, 263

Christopher, V, and Roberts, N, J, 'William H.F. Fitzpatrick's Editorials on Human Rights (1994)' < https://www.geschichte–menschenrechte.de/schluesseltexte/william–h–fitzpatricks–editorials–on–human–rights–1949 > accessed 2 April 2021.

Chuma–Okoro, H 'The Nigerian Constitution, the ECOWAS Treaty and the Judiciary: Interplay of Roles in the Constitutionalisation of Free Trade (2020) 4(1) Global Journal of Comparative Law, 43.

Citron, K, D 'Mainstreaming Privacy Torts' (2010) 96(6) California Law Review, 1805–1852.

Clarke, A, 'International Instruments Relating to Privacy Law' < http://www.rogerclarke.com/DV/PLawsIntl.html > accessed 18 April 2021.

Clarke, R, Introduction to Dataveillance and Information Privacy and Definition of Terms (1997) < http://www.rogerclarke.com/DV/Intro.html> accessed 28 March 2021.

Clarke, R, What is Privacy (2006) < http://www.rogerclarke.com/DV/Privacy.html> accessed 29 March 2021.

Cleber Sanfelici and Lucimare Plaza Tena, 'The Reasons that Justify the Rights of Privacy: Human Dignity as the core of Personality Rights and Situations at Density that Allow Flexibility' (2016) 11(2) DOAJ, 476–498.

Clifford, D, 'Fairness and the General Data Protection Regulation– Operationalising Fairness in Data Protection Impact Assessments' Report Commissioned by Office of Data Protection officer at Facebook < https://hmi.anu.edu.au/ourwork/fairness–and–the–general–data–protection–regulation> accessed 19 June 2021.

Clifford, D, and Ausloos, J, 'Data Protection and Rule of Fairness' (2018) 37(1) Yearbook of European Law, 130–187.

Cohen, E, J, Intellectual Privacy and Censorship of the Interest (1998) 8 Seton Hall Const. L.J. 693.

Cohen, J, What Privacy is for? (2013) 126 Harvard Law Review, 2.

Convery, A, M, 'The Privacy of Telephone Conversations under German Law and Article 8 of the European Convention of Human Rights: Improving Human Rights Enforcement Through Domestic Decisions' (1995) 38 German Y.B. Int'l 153.

Cooley, M, T, A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract (Callaghan and Company 1879).

Cramer, R. D, 'Images of home' (1960) XLVI Journal of the American Institute of Architects, pp. 40–49.

Cranor, L, F, Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2013) 10 Journal on Telecommunications and High Technology Law, 10, 273–308.)

Cuijpers, C, 'A Private Law Approach to Privacy: Mandatory Law Obliged' (2007) 4/4 SCRIPT ed 304–18 at 312.

Custers, B & Ursic, H 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6(1) International Data Privacy Law, 4–15.

Da Silva, R, B 'Taxonomy and typology: Are they really synonymous?' (2014) 25(5) Santé Publique, 633–7.

Dada, A, J, 'Human Rights Protection in Nigeria: The Past, the Present and Goals for Role Actors for the Future' (2013) 14 Journal of Law, Policy and Globalization, 4.

Dalenius, T, 'Data Protection Legislation in Sweden: A Statistician's Perspective' (1979) 142(3) Journal of the Royal Statistical Society, 285–298.

Dan Jerker Svantesson–Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5(4) International Data Privacy Law, 233.

De Hert, P and Gutwirth, S, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Privacy and the Criminal Law Serge Gutwirth, Anthony Duff and Erik Claes(eds) (Intersentia, 2006.) 1.

De Hert, P and Schreuders, E, 'The Relevance of Convention 108' 33,42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw 19–20 November 2001.

De Hert, P and Serge Gutwirth, Data Protection in the Case Law of Strasbourg and Luxembourg: Constitution in Action in

Reinventing Data Protection? (Springer, 2009) 3.

De Hert, P et al, 'The Right to Data Portability in the GDPR: Towards User Centre Interoperability of Digital Services' (2018) Computer Law & Security Review, 193–293.

Desmond, A, 'The Private Life of Family Matters: Curtailing Human Rights Protection for Migrants under Article 8 of the ECHR?' (2018) 29(1) European Journal of International Law, 261–279.

Diggelman, O, and Cleis, M, N, 'How the Right to Privacy Became a Human Right' (2014) 14 Human Rights Law Review, 441–458.

Dolinger, J, 'The failure of the Universal Declaration of Human Rights' (2016) 47 University of Miami Inter American Law Review 184.

Dorfleitner, G, and Hornuf, L, Fintech and Data Privacy in Germany (Springer, 2020)

DPAs are meant to provide 'expert advice' on data protection matters, issue guidance notes and inform the public on their rights and obligations under the relevant data protection laws. While NITDA may claim to perform some of these roles, the NDPR is not clear on them. For more reading on roles of DPAs, see Peter Hustinx, 'The Role of Data Protection Authorities' in Reinventing Data Protection? Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds) (Springer, Dordrecht, 2009) 133.

Ducato, R 'Data Protection, Scientific Research and the Role of Information' (2020) 37 Computer law and Security Review,1, 8.

Duckham, M, and Kulik, L, Location Privacy and Location Aware Computing <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.366.1455&rep=rep1&type=pdf> accessed 29 March 2021.

Duropthy J. Glancy, 'The Invention on Right to Privacy' (1979) 21(1) Arizona Law Review, 2.

Dworkin, R, Taking Rights Seriously (Harvard University Press, 1971) 262.

Edosomwan, U, C Power of the Nigeria Attorney General in Perspective' in The Attorney General: Chronicles and Perspectives Olumide Babalola (ed) (Law Pavilion, Grace Info Tech Ltd, 2013) 30.

Elgujja, A, A, 'A Synopsis on Data Protection Under the Nigerian Laws: Has the Universality of Right to Privacy Tricked Down to Nigeria? (2020) < https://osf.io/fk5xg > accessed 12 April 2021.

Elizabeth Anne Kirley, Reputational Privacy and the Internet: A Matter for Law? (2015) published PhD thesis Osgoode Hall Law School, York Univeristy, 2015.

Enabulele A 'The Right to life or the Right to Compensation Upon Death: Perspectives on an Inclusive Understanding of the Constitutional Right to Life in Nigeria' (2014) 3(1) Afe Babalola University, Journal of Sustainable Development Law and Policy, 100, 111.

Enakhire, R, T 'The Nigerian National Information Technology (IT) Policy' in Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements' in

‘Information Science Reference Eshareniana E. Adomi (ed.) (New York, 2011)

Eton O’Dell, ‘Compensation for Breach of the General Data Protection Regulation’ (2017) 40(1) Dublin University Law Journal, 97–164.

Etzioni, A and. Rice, J, C ‘Privacy in a Cyber Age: Policy and Practice’ (Palgrave Macmillan London, 2015) 73;

European Data Protection Supervisor, ‘Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data (EDPS) (2016) Opinion 8/2016 8 < https://edps.europa.eu/sites/default/files/publication/16–09–23_bigdata_opinion_en.pdf> accessed 10 May 2021.

European Data Protection Supervisor, ‘Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001’ (2005) https://edps.europa.eu/sites/edp/files/publication/05–11–28_dpo_paper_en.pdf accessed 1 July 2021.

Fabiano, N, Ethics and the protection of personal data, (2019) IMCIC 2019–10th International Multi–Conference on Complexity, Informatics and Cybernetics, Orlando, Florida, USA, 1–17.

Felzmann, H, Villarionga, E, Lutz, F and Aurelia Tamo–Larrieux ‘Transparency You Can Trust: Transparency Requirement for Artificial Intelligence Between Legal Norms and Contextual concerns’ (2019) Big Data & Society 1, 2.

Ferdinand J. Jr. Zeni, Wiretapping–The Right of Privacy versus the Public Interest’ (1950) 40(4) Journal of Criminal Law and

Criminology, 476.

Ferreti, F, 'Data Protection and the Legitimate Interest of Data Controllers:) Much Ado About Nothing or The Winter of Rights' (2014) 51 Common Market Law Review, 846

Ferretti, F, EU Competition Law, the Consumer Interest and Data Protection: The Exchange of Consumer Information in the Retail Financial Sector (Springer, 2014) 105.

FHC/AB/CS/85/2020 (Abeokuta division)

Finck, M and Pallas, F 'They Who Must Not Be Identified–Distinguishing Personal from Non–Personal Data Under the GDPR' (2020) 10(1) International Data Privacy Law, 11,13.

Finn, L, R, Friedewid, M, and Wright, D, Seven Types of Privacy in European Data Protection: Coming of Age, Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet (eds) (Springer, 2013).

Fitzjames, J, Stephen, Liberty, Equity Fraternity (London Smith, Elder & Co 1873). See also H.J. McCloskey 'Privacy and the Right to Privacy' (1980) 55 (211) Cambridge University Press, 17–38.

Floridi, L, Fourth Revolution (Oxford University Press, 2014) 272.

Floridi. L, The Ethics of Information (OUP Oxford, 2013) 257.

Forde, A, 'The Conceptual Relationship Between Privacy and Data Protection' (2016) 1 Cambridge Law Review, 140.

Fox, L 'The Meaning of a Home: A Chimerical Concept or Legal

Challenge' (2002) 29(4) Journal of Law and Society 580–610.

Foxley v United Kingdom (no. 33274/96. 20 June 2000.

Fried, C, Privacy (1968) 77(3) The Yale Law Journal 475–493.

Friedman, B, Felten, E and Millett, I' L "Informed Consent Online: A Conceptual Model and Design Principles" < ftp.cs.washington.edu › 2000/12 › UW–CSE–00–12–02> accessed 28 May 2021.

Fuster G, G 'How Informed is the Average Data subject? A Quest for Benchmarks in EU Personal Data Protection' (2014) IDP Revista de Internet, Derecho y politica, 92.

Fuster G, G, and Gellert, R, 'The Fundamental Right of Data Protection in the European Union: In search of an Uncharted Right'. (2012) 26(1) International Review of Law, Computers & Technology, 73–82 and

Fuster, G, G, The Emergence of Personal Data Protection as a Fundamental Right of the European Union (Springer, 2014) 1.

Fuster, G, G, 'Transparency as Translation in Data Protection' in Being Profiled: Logitas Ergo Sum: 10 Years of Profiling the European Citizen, Emre Bayamilogu, Irina Baraliuc, Liisa Albertha Wilhelmina Janssens and Mireille Hilderbrandt, (eds) (Amsterdam University Press, 2018).

Fuster, G, G, de Hert, P, and Gutwirth, S, 'The Law–Security Nexus in Europe: State of the Art Report' (2008) Report submitted in fulfilment of Requirements of the FP7 Project Converging and Conflicting Ethical Values in the International Security Continuum in Europe (INEX) WPZ D21, 11.

Garba, 'Permissible Limitations to Freedom of Religion and Belief in Nigeria' (2020)15 Religion and Human Rights, 57–76.

Garner, A, Black's Law Dictionary, (11 edn, Thomson Reuters, 2019) 1929.

Gellert, R, 'Understanding Data Protection as a Risk Regulation' (2015) 18(11) Journal of Internet Law, 3–16.

Gerety, T, Redefining Privacy (1977) 2 Harv CRCLL Rev.233 at 236

Giakoumopoulos, C, Buttarelli, G and O'Flaherty, M *Handbook on European Data Protection Law, (*2018 edn, European Union Agency for Fundamental Rights and Council of Europe) 151.

Gilardi, F 'Policy Credibility and Delegation to Independent Regulatory Agencies: A Comparative Empirical Analysis' (2002) 9 Journal of European Public Policy, 873–893.

Glendeon, A, G, The Rule of Law in the Universal Declaration of Human Rights' (2004) 2(1) North Western Journal of International Human Rights, 4.

Goldim, R, J and Gibbon, S, Between Personal and Relational Privacy: Understanding the Work of Informed Consent in Cancer Genetics in Brazil (2015) 6(3) Journal of Community Genetics, 287–293;

Goliker, P 'A Common Law Tort of Privacy? The Challenges of Developing a Human Rights Tort' (2015) 27 Singapore Academy of Law Journal, 711–788.

Gomes de Andrade, N, N. 'Data Protection, Privacy and Identity:

Distinguishing Concepts and Articulating Rights' in Privacy and Identity Management for life (1st edn, Springer, 2011) 96

Greenleaf, G and Cottier, B, Comparing African Data Privacy Laws: International, African and Regional Commitments, (2020) University of New South Wales Law Research Series, 32.

Greenleaf, G, 'The 1995 EU Data Protection Directive on Data Protection. An Overview' (1995) 3(2) International Privacy Bulletin, 1–21.

Greenleaf, G, How Far Can Convention 108 Globalise? Prospects for Asian Accessions,' (2020) Computer Law & Security Review, 3.

Guadamuz, A 'Developing a Right to be Forgotten' in EU Internet La, Regulation and Enforcement (Springer, 2017) 2.

Gutwirth, S, Privacy and the Information Age (Lenham, MD Lovren & Littlefield, 2002) 30.

Hafetz, L, J 'A man's Home is His Castle? Reflections on the Home, the Family and Privacy During the Late Nineteenth and Early Twenties Centuries' (2001–2002) 8(2) William & Mary Journal of Women and the Law, 175.

Hallinan, D and Borgesius, Z, F 'Opinions can be incorrect (In our Opinion) on Data Protection Law's Accuracy Principle' (2020) 10(1) International Data Privacy Law, 1,

Harbinja, E, Post–Mortem Privacy 2.0: Theory, Law, and Technology (2017) 31(1) International Review of Law, Computers & Technology, 26–42

Hargreaves, S, Relation Privacy and Tort (2017) 23 (3) William and Mary Journal of Women & the Law, 433.

Harland, C, 'The Status of the International Covenant on Civil and Global Survey Through UN Human Rights Committee Documents' (2000) 22(1) Human Rights Quarterly, 187–260.

Henry, L 'Information Privacy and Data Security' (2015) Cardozo Law Review de Novo, 107, 111.

Herman T. Tavani, 'Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy' (2007) 38(1) Metaphilosophy, 1–22.

Hill, A, C and Scudder, D, G 'The use of Electronic Data interchange for Supply Chain Coordination in the Food Industry; (2002) 20 Journal of Operations Management 375–387.

Holvast, J, History of Privacy in the future of Identity in the Information Society, Vashek Matyas, Simone Fisher–Hubner & Petr Svenda (eds) (2008) 298 IFP Advances in Information Communication Technology, 1.

Hondius, F, 'Emerging Data Protection in Europe (North–Holland Pub. G: American Elsevier Pub. Co. 1975), 1.

Hoofnagle, J, C, Sloot, B, Borgesius, Z, F 'The European Union General Data Protection Regulation: What it is and What it Means? 28(1) Information & Communications Technology Law, 65–98;

Hornung, G, and Schnabel, C, 'Data Protection in Germany I: The Population Census Decision and the Right to informational Self–Determination' (2009) 25(1) Computer Law & Security

Report, 84–88.

Hyman Gross, 'the concept of privacy (1967) 42(1) NY Univ.L. Rev. 30,35–36).

Ibidapo–Obi, A, Essays on Human Rights Law in Africa (Concept Publications Ltd, 2005)

Ijewere, A, A, and E.C. Gbandi, 'Telecommunications Reform in Nigeria. The Marketing Challenges (2012) 10(2) JORIND 194.

Inness, J, Privacy, Intimacy and Isolation (Oxford University Press, New York, 1992).

Iwobi, U, A, 'Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime' (2016) 26(3) Transnational Law and Contemporary Problems 13.

Iwuugwu, E, K 'The Concept of Citizenship; Its Application and Dental in the Contemporary Nigerian Society' (2015) 8(1) International Journal of Research in Arts and Social Sciences, 165.)

J. Sturgess, J.R.C. Nurse and J. Zhao, 'A Capability Oriented Approach to Assessing Privacy Risk in Smart Home Ecosystems' (2018) Conference paper at Living in the Internet of Things. Cybersecurity of IOT.

Jacobson, A, Boldt, M, and Carlsson, B, 'A Risk Analysis of a Smart Home Automation System (2016) Future Generation Computer Systems, 719–733.

James Fitzjames Stephen, 'Liberty, Equality, Fraternity (1st ed.

1873).

Jasmontaite, L and Verdoodt V 'Accountability in the EU Data Protection Reform: Balancing Citizens' and Business Rights' (2016) in Privacy and Identity Management. Time for a Revolution? Privacy and Identity 2015,476 IFCP Advances in Information and Communication Technology, 156–169.

Jasserand, C 'Legal Nature of Biometric Data: From 'Generic' Personal Data to sensitive Data' (2016) 2(3) Eur. Data Protection Law Revision, 297.

Jemilohun, O, B, and Akomolede, I, T 'Regulations or Legislation for Data Protection in Nigeria? A Call for a Clear Legislative Framework' (2015) 3(4) Global Journal of Politics and Law Research, pp.1–16.

Jensen, C, M 'The Modern Industrial Revolution, Exit and the Failure of Internal Control Systems' (1993)48 Journal of Finance, 831–880.

Jens–Erik Mai, 'Three Models of Privacy, New Perspectives on Informational Privacy' (2016) 37(1) Nordicom Review 171–175

Jerome Richman and Pamela Samuelson 'Intellectual Property Rights in Data?' (1997) 50 Vand. L. Rev. 51.

John P. Humphrey, 'The International Bills of Rights: Scope and Implementation' (1976) 17(3) William & Mary Law Review, 528.

Judith De Cew, 'Privacy' (2018) The Stanford Encyclopedia of Philosophy, <https://plato.stanford.edu/entries/privacy/> accessed 3 April 2021.

Judith Jarvis Thompson, The Right to Privacy' (1975) 4(4) Philosophy & Public Affairs, 295.

Justice Cooley, M, T, A Treatise of the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union (4th edn, Brown & Co. Boston, 1871).

Kadam, A, R 'Informed consent process: A step further towards making it meaningful!' (2017) 8(3) Perspect Clinical Research, 107–112.

Kakabadse, A, and Kakabadse, N, 'Chairman and Chief Executive Officer (CEO): That Sacred and secret Relationship' (2006) 25(2) Journal of Management Development, 150.

Kalhan, A, 'The Fourth Amendment and Privacy: Implications of Interior Immigration Enforcement' (2008) U.C. Davis Law Review, 41 pp 113 217.

Kaltheuner, E & Bietti, E 'Data is Power: Towards Additional Guidance on Profiling and Automated Decision–Making in the GDPR' (2018) 2(2) Journal of Information Rights Policy and Practice, 1.

Kamara, I and Hert, P 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach' (2018) 4(12) Brussels Privacy Hub, 12.

Kaner, C, Bygrave, L, Dicksey, C and Drechesler, L The EU General Data Protection Regulation (GDPR). A Commentary' (Oxford university Press, 2020) 183.

Karyda, M and Mitrou, L, Data Breach. Notification issues and

Challenges for Security Management (2016) Tenth Mediterranean Conference on Information System (MCIS) Paphos, Cyprus, September 2016.

Kekey, G, P, Cesca, L, Biesse & Loririe Faith Crenor, 'Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach' (2009) The Proceedings of the 28th International Conference on Human Factors in Computing Systems, CHI 2010, Atlanta Georgia, USA, April 10–15, 2010.

Khazanchi, D 'An Empirical Analysis of Benefits of Electronic Data Interchange (EDI) Implementation: Implications for New IT Implementation' (2002) 13(1) Journal of Small Business Strategy, 46.

Kilkelly, U, 'The Right to Respect for Private and Family Life' Human Rights Handbook No.

Kim Lane Scheppele, Legal Secrets, Equality and Efficiency in the Common Law (University of Chicago Press 2020).

Kirwan, et al, M 'What GDPR and Health Research Regulations (HRRs) Mean for Ireland: "Explicit Consent"–a Legal Analysis' (2020) 110 Irish Journal of Medical Science, 517.

Klifou, D, Privacy–Invading Technologies and Privacy by Design (Spinger, 2004)

Kloza, D and Moscibroda, A 'Making the Case for Enhanced Enforcement Cooperation Between Data Protection Authorities: Insights from Competition Law' (20214) International Data Privacy Law 4(2) 120, 121.

Klug, C's, Book Review 'Spiros Simitis, Bundesdatenschutzgesetz, 7th edn (in German), Nomos, 2011, 1,886 pp, hdbk, E178, ISBN 978 –3 –8329 –4183 –3' (2012) 2(2) International Data Privacy Law, 113.

Korff, D and Marie Georges, 'The Origins and Meaning of Data Protection' (2020) <https://ssrn.com/abstract=3518386> accessed 7 April 2021.

Kosta, E, Consent in European Data Protection Law, (Martinus Nijhoff Publishers, 2013) 46.).

Krishnamurthy. V, 'A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy' (2020) 114 AJIL Unbound, 26–30

Kristen D.A. Carpenter, 'The International Covenant of Civil and Political Rights: A Toothless Tiger' (2000) 26(1) North Carolina Journal of International Law and Commercial Regulation, 1.

Kulver, Jr., H 'Privacy in Tort Law–Were Warren and Brandeis Wrong' (1966) 31 Law and Contemporary Problems 326–341.

Kuner C 'The Court of Justice of the EU Judgement on Data Protection and Internet Search Engines' (2015) LSE Law Society and Economy Working Papers 3/2015.

Kuner, C 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past Present and Future' (2011) OECD Digital Economy Papers No 187, OECD Publishing.

Kuner, C, 'Transborder Data Flows and Data Privacy Law (Oxford University Press, 2007) 1; (De Hert, P and Eric Schruders, 'The Relevance of Convention 108' 33, 42 Proceedings of the Council

of Europe Conference on Data Protection, Warsaw November 19–20, 2001.

Kuner, C, Bygrave, A, L, Polksey, C and Drechsler, L The *EU General Data Protection Regulation (GDPR) A Commentary* (Oxford University Press, 2020) 333.

Kuner, C, Transborder Data Flows and Data Privacy (Oxford Scholarship Online, 2003)

Lachaud, E 'Astering to GDPR codes of Conduct: A possible Option for SMEs to GDPR Certification' www. Accessed 2 May 2020.

Lachaud, E 'What GDPR Talks About Certification (2020) 38 Computer Law and Security Review, 1.

Lafley, G, A what only the CEO Can Do (2009) 87(5) Harvard Business Law Review, 54–62.

Lambert, P, *The Data Protection Officer: Profession, Rules and Role* (Auerbach Publications, 2017) 20.

Langhanke, C and Schmidt–Kessel, M 'Consumer Data as Consideration' (2015) 4(6) Journal of European Consumer and Market Law 218–223.

Lanzing, M, 'Strongly Recommended' Revisiting Decisional Privacy to Judge Hper nudging in Self Tracking Technologies' (2019) 32 Philosophy Technology, 549–568.

Lateef, A, M and Taiwo, O, I 'Examination of the Legal Regime for Information Privacy, Data Protection and Enforcement of Sanctions in Nigeria' (2020) 3 Elizade University Law Journal,

151, 184.

Lindgren, C–J and Folkerts–Landau, D.F.I 'Supervisory Oversight' in Towards a Framework for Financial Stability (International Monetary Fund, 1998).

Liu, F, P, Vitak, J, and Zimmer, T, M, A Contextual Approach to Information Privacy Research (2019) 4 Journal of the Association for Information Science and Technology, 1.

Lukacs, A, What is Privacy; The History and Definition of Privacy (2016) University of Szeged 16

Lundgren, B, A Dilemma for Privacy as Control' (2020) 24 The Journal of Ethic, 165–175.

Lydia F. de la Tore, 'What Does Lawfulness, Fairness and Transparency mean under EU Data Protection Law' (2019) < https://medium.com/golden–data/what–does–lawfulness–fairness–and–transparency–mean–under–eu–dp–law–a385d249d754 > accessed 11 May 2021.

Lynn, T, Mooney, Lisa van der Werff and Grace Fox, Data Privacy and Trust in Cloud Computing (Palgrave Mcmillan, 2020).

Lynskey, O, 'Deconstructing Data Protection; The Added Value of a Right to Data Protection in the EU Legal Order' (2015)63 International &Comparative Law Quarterly, 590

Lynskey, O, Orla, The Foundations of EU Data Protection Law (1st edn. Oxford University Press, 2005) 260;

Magdalene Jozwiak, 'Balancing the Rights to Data Protection and

freedom of Expression and Information by the Court of Justice of the European Union' (2016) 23(3) MJ, 404.

Makulilo, A, A Person is a Person Through Other Persons'–Critical Analysis of Privacy and Culture in Africa' (2016) 7 Beijing Law Review 192–204.

Makulilo, A, African Data Privacy Laws (Springer, 2016); Nora Ni Loideain EU Data Privacy Law and Serious Crime (Oxford University Press, 2020).

Makulilo, A, B, 'The Quest for Information Privacy in Africa' (2018) 8 Journal of Information Policy, pp. 317.

Makulilo, B, A 'Myth and Reality of Harmonization of Data Privacy in Africa' (2015) 31(1) Computer Law and Security Review, 78–89.

Makulilo, B, A, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law, 165.

Malatras, A, Sanchez, I, Beslay, L, Coisel, I ,Vakalis, L, D'Acquisto, G, Sanchez, M, Grall, M, Hansen, M and Zorkadis,V 'Pan European Data Breaches: Mapping of Current Practices and Recommendation to Facilitate Cooperation Among Data Protection Authorities' (2017) 33 Computer Law & Security Review, 458–469.

Malgieri, M, 'The Concept of Fairness in the GDPR' A Linguistic and Contextual Interpretation' (2020) Proceedings of the 2020 Conference in Fairness, Accountability and Transparency, 154–166.

Mall, L, L, 'The Right to Privacy in Great Britain: Will Renewed Anti–Media Sentiment Compel Britain to Create a Right to Be

Let Alone' (1998) 4 (2) ILA Journal of International Comparative Law, 35.

Margulis, S, Privacy as Social Law and Behaviour Concept' (2003) 59(2) J.Soc. 244.

Margulis, T, S, Conceptions of Privacy: Current Status and Next Steps 33(3) Journal of Social Issues, 5–21.

Markesinis, B, O'Cinneide, 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(1) The American Journal of Comparative Law, 133–208.

Marmor, A, What is Right to Privacy? (2015) 43(1) Philosophy & Public Affairs, 3–26.

Masciandaro,D, Quintyn, M and Taylor, M 'Financial Supervisory Independence and Accountability–Exploring the Determinant' (2008) IMF Working Paper, 1, 5.

Matheson, D, A Distributive Reductivism About the Right to Privacy' (2008) 9(1) The Monist, 108–129; Robert Posner, The Economics of Justice (Hup, Cambridge 1981)

Maxmilian von Grafenstein, The Principle of Purpose Limitation in Data Protection Laws (Nomos Verlagsgeselischaft mbH, 2018) 31.

Mayer–Schönberger, V, "Generational Development of Data Protection in Europe," in P. E. Agre & M. Rotenberg (Eds.), Technology and Privacy: The New Landscape, London: MIT Press, 1998) at 219–241.

Mba, O 'Judicial Review of the Prosecutorial Powers of the Attorney General in England and Wales and Nigeria

McCloskey, H, J, Privacy and the Right to Privacy (1980) 55 (211) Cambridge University Press, 17, 23.

Mintzberg, H, The Nature of Managerial Work (New York, Harper Row, 1973).

Moerel, M and Storm, M 'Automated Decision Based on Profiling. 'Information, Explanation or Justification' that is the Question' in *Autonomous Decisions and the Law* Nikita Aggarwal, Horst Eidenmuller, Lucas Enriques, Jennifer Pyne, Kristin van Zwieten (eds) (C.H Beck, Nomos, 2019) 1.

Mondschein, F, C and Monda, C 'The EU's General Data Protection Regulation (GDPR) in a Research Context' in Fundamentals of Clinical Data Science, Pieter Kubben, Michel Dumontier, and Andre Dekker (eds) (Springer, 2019) 62.

Moore A, Defining Privacy (2008) 39(3) Journal of Social Philosophy) 411–428.

Moreham, A, N, Beyond Information; Physical Privacy in English Law (2014)73(2) The Cambridge Law Journal 359.

Moreham, A, N, Privacy in Public Places (2006) 65(5) The Cambridge Law Journal, 606–635.

Mourby et al, M 'Are Pseudonymized Data Always Personal Data? Implications of the GDPR for Administrative Research in the UK' (2018) 34 Computer Law &Security Review, 222–233.

Natelson, R, G, 'Founding–Era Socialism; The Original Meaning of the Constitution Postal Clause' (2018) 7(1) British Journal of American Legal Studies, 15.

Norberg–Schulz, C, Loci, G, Towards a Phenomenology of Architecture (New York Rizzoli,1980).

Nos. 33677/10 and 52340/10.

Nwabueze, B A Constitutional History of Nigeria, (Longman, New York, 1982) 18.

Nwafor, O, A, 'Enforcing Fundamental Rights in Nigerian Courts–Processes and Challenges' (2009) 4 African Journal of Legal Studies 1–11.

Nwalimu, C, Nigerian Legal System (Vol 1. Peter Lang Publishing, New York, 2007)

Nwankwo, B, 'The Status of Data Protection Reform in Nigeria' (2015) https://iheanyisam.wordpress.com/2015/02/25/the–status–of–data–protection–reform–in–nigeria/ accessed 16 March 2021.

Nwankwo, B, 'Nigeria's Data Privacy First Responders' (2018) < https://iheanyisam.wordpress.com/2018/04/04/nigerias–data–privacy–first–responders/> accessed 18 March 2021.

Nwauche, S, E, 'The right to privacy in Nigeria (2007)1 CALS review of Nigerian Law and practice, 64, 65.

Nxumalo, c, Z, Tarwireyi, P, Adigun, O, M 'Towards Privacy with Tokenization as a Service' (2014) IEEE with International

Conference on Adaptive Science & Technology (ICAST) 1–6.

Oakley, O 'What is E–Governance' (2010) Integrated Project 1. e–Governance Workshop, Strasbourg, 10–11.

Obi, V, U, 'An Extensive Article on Data Privacy and Data Protection Law in Nigeria' (2020)

Ogbu, O, Human Right Law and Practice, (2nd edn, Snaap Press, Enugu, 2013) 280–281.

Ogunfuwa, I, 'Experts Call on Buhari to Assent Data Protection Bill' (2020) < https://punchng.com/experts–call–on–buhari–to–assent–data–protection–bill/> accessed 1 March 2021.

Ojo, S, J 'Root Development in Nigeria' (2014)6(4) Journal of Public Administration and Policy Research, 78.

Olinger, H, Britz, J, & Olivier, B, Wester Privacy and/or Ubuntu? Some Critical Comments or the influence in the forthcoming Data Privacy Bill in South Africa (2007) 39 (1) International information & Library Review, 31.

Olomojobi, Y, Right to Privacy (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062603> accessed 29 March 2021.

Olubusoye, O, Korter, G, and Keshinro, O, 'Nigerian Statistical System; The Evolution, Progress and Challenges' (2015) < https://www.researchgate.net/publication/283715250_NIGERIAN_STATISTICAL_SYSTEM_THE_EVOLUTION_PROGRESS_AND_CHALLENGES >accessed 5 April 2021.

Oman, S, 'Implementing Data Protection in Law' (2004) 47

Scandinavian Studies in Law, 389–403.

Omotubora, A, & Basu, S 'Next Generation Privacy' (2020) 29(2) Information & Communications Technology Law' 151–173.

Onuigbo, A, R and Eme, I 'Electronic Governance and Administration in Nigeria: Prospects and Challenges' (2015) 5(3) Arabian Journal of Business and Management Review, 18.

Orji, J, U, 'A Comparative Review of the ECOWAS Data Protection Act' (2016) 17(4) Computer Law Review International, 108.

Osakede, K, Ijimakinwa, S and Adesanya, T 'Local Government Financial Autonomy in Nigeria: An Empirical Analysis' (2016) 5(11) Kuwait Chapter of Arabian Journal of Business and Management Review 24, 29.

Osemwuta, O, E and Agbebuku, P 'Autonomy and Local Capacity. An Analysis of the Performance Profile of Edo State Local Government Councils' (2011) 6(3) Mendrell Journals, The Social Science, 235–236.

Oulasvirta, L and Turala, M 'Financial Autonomy and Consistency of Central Government Policy Towards Lord Governments' (2009) 75 International Review of Administrative Sciences, 311.

Palvia, S and Sharma, S 'E–Government and E–Governance: Definitions/Domain Framework and Status Around the World' (2007) Computer Society of India, 3.

Pamela Samuelson, 'Privacy as Intellectual Property' (2000) 52(5) Stanford Law Review, 1125–1173.

Paolo Guarda, 'Data Protection, Information Privacy, and Security Measures: An Essay on the European and the Italian Legal Frameworks'(2008)<https://core.ac.uk/download/pdf/150082461.pdf> accessed 12 April 2021

Parker, R, A Definition of Privacy (1st edn Routledge, 2001) 1.

Paul Freund, Privacy: One Concept or Many in Privacy & Personality (1st edn Routledge, 1971).

Petkovska, S 'An Analysis of financial Autonomy in Macedonian Higher Education' (Master's Thesis, University of Avaro, 2011).

Phillipson, G, 'Transforming Breach of confidence? Towards a Common Law Right of Privacy under Human Rights Act? (2003)66(5) The Modern Law Review 726–758

Piatek, W 'The Right to an Effective Remedy in European Law: Significance, Content and Interaction' (2019) 6 China–EU Journal, 163–174.

Pillai, G, Indian Constitutional Law and Philosophy (2019) <https://indconlawphil.wordpress.com/tag/abortion/> accessed 28 march 2021.

Porcedda, G, M Data Protection and the Prevention of Cybercrime; The EU as an Area of Security? (2012) EUI working Paper Law 2012/25.

Pormeister, K 'Informed Consent to Sensitive Personal Data for the Performance of Digital Consumer Contracts on the Example of 23 and Me' (2017) 6(1) J. Eur. Consumer & MKT. L, 17.

Posner, R, The Economic of Justice (Harvard University Press 1981)

Powers, S, 'Where did the Principle of Secrecy in Correspondence Go? (2015) The Guardian < https://www.theguardian.com/technology/2015/aug/12/where–did–the–principle–of–secrecy–in–correspondence–go> accessed 10 April 2021.

Pratikto, Y, R, Santoso, B, P and Sugiono, S 'A Literature Review of Electronic Data Interchange as Electronic Business Communication for Manufacturing' (2018) 9(4) Management and Production Engineering Review, 117–128.

Premkumar, P, Ramamurthy, R and Nilakanta, S 'Implementation of Electronic Data Interchange: An Innovation Diffusion Perspective' (19941)11(2) Journal of Management Information Systems, 157–186.

Proehl, O, P, Fundamental Rights Under the Nigerian Constitution, 1960–1965 (1970) 8 Occasional Paper, African Studies Centre, University of California, 6.

Prosser, L, W 'Privacy' (1960) 48(3) California Law Review, 385.

Quinn, P and Malgieri,G 'The Difficulty in Defining Sensitive Data' (2020) German Law Journal, 1.

Raab, C 'The Meaning of Accountability in the Information Privacy Context' in Managing Privacy Through Accountability Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener & Hector Postigo (eds) (Palgrave and Macmillan, 2012) 27.

Raab, D, C 'The Governance of Global Issue: Protecting Privacy

in personal information in New Modes of Governance in the Global System International Policy Economy Serves (Palgrave Macmillan, London 2006.

Ramezani et al, Z 'Use of Mintzberg's Model of Managerial Roles to Evaluate Sports Federations Managers of Iran' (2011)10(5) Middle East Journal of Scientific Research, 559–564.

Rao, S, H, K, 'Informed Consent: An Ethical Obligation or Legal Compulsion' (2008)1(1) Journal of Cutaneous Aesthetic Surgery, 33–35.

Recio, M 'Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability' (2017) 3(1) European Data Protection Law Review, 114.

Refat Al–Sohan, 'Why Should Right to Privacy Be a Human Right?' < https://www.researchgate.net/publication/328725112_Why_Should_Right_To_Privacy_Be_A_Human_Right> accessed 11 April 2021.

Reidenberg, R, J, Privacy in Public (2014) 69 U. of Miami L. Rev. 141.

Rengel, A, 'Privacy as an International Human Right and the Right to Obscurity in Cyber space' (2014) 2(2) Groningen Journal of International Law, 34.

Richard, M, N, and Solove, J, D Prosser's Privacy Law: A Mixed Legacy' (2010)98(6) California Law Review, 1887–1924

Richards, N, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (Oxford University Press, 2017).

Riley, B, T Electronic Governance in Context, Electronic Governance and Electronic Democracy: Living and Working in connected World (Commonwealth Secretariat, 2000).

Roger J.R. Lavesque, Adolescence, Privacy and the Laws: A Developmental Science Perspective, (Oxford Scholarship Online, 2016).

Rogers, H, "Is there a right to reputation?" (2010) < https://inforrm.wordpress.com/2010/10/26/is–there–a–right–to–reputation–part–1–heatherrogers–qc/> accessed 2 April 2021.

Roos, A, 'Core Principle of Data Protection Law' (2006) 39(1) Computer and International Law Journal of Southern Africa 102–130.

Rossler, B, The Three Dimensions of Privacy in The Handbook of Privacy Studies, Bart van der Sloot and Aviva de Groot (eds) (Amsterdam University, Press 2018).

Rumbold, B and Wilson, J, 'Privacy Rights and Public Information' (2019) 27(1) The Journal of Philosophy and Public Affairs 269–288; William A. Parent, 'Privacy, Morality and the Law' (1983) 12 Philosophy and Public Affairs, 269–288.

Sacharoff, L, The Relational Nature of Privacy (2013) 16(4) Lewis & Clark Law Review 1249.

Salami, E The Nigerian Data Protection Regulation: Overview, Effects and Limits' (2019) < https://www.datenschutz–notizen.de/the–nigerian–data–protection–regulation–2019–overview–effects–and–limits–3522349/> accessed 10 April 2021.

Sallinen and Others v Finland no.50882199, 71, 27 September 2005 and Case of Wiesner and Bicos Beteileigungen GmbH v Austria no. 74336101, 16 January 2008.

Sandru, M–D, 'The Fairness Principle in Personal Data Processing' (2019) 10(2) Law Review 60,61.

Sang, P, M Democracy in Nigeria (1958) 9 (2) National Black Law Journal, 129.

Saruwono, M, 'Shouting in Silence: Expression of Self in Private Homes' (2021) 42 Procedia Social and Behavioural Sciences.

Schermer, W, B, Custers, B and Hof, S 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014)11 Ethics Information Technology, 173.

Schoeman, F, Privacy: Philosophical Dimension of the Literature in Philosophical Dimensions of Privacy: An Anthiology. Federick Schoeman (ed) (Cambridge University Press, 1984) 1.

Scholz, H, L. Information Privacy and Data Security (2015) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2600495> accessed 11 April, 2021.

Schutz, P 'Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective' (2011) 7th Prime Life International summer school, Trento, Italy, 45–58.

Scutariu, Aand Scutariu, P 'The Lines Between Financial Autonomy and Local Development. The Case of Romania' (2015) 32 Procedia Economic & Finance, 542.

Seinen, W, Walter, A, and Sari van Grondelle, 'Compatibility is a Mechanism for Responsible Further Processing of Personal Data' https://www.bakermckenzie.com/–/media/files/insight/publications/2018/10/compatibility_mechanism_responsible_further_personal_data_processing.pdf?la=en > accessed 12 June 2021.

Selbst, D, A, and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7(4) *International Data Privacy Law*, 233–242.

Sen, R & Borle, S, Estimating the Contextual Risk of Data Breach: An Empirical Approach (2015) 32(2) Journal of Management Information Systems, 314–341.

Senz, D and Charlesworth, H, 'Building Blocks: Australia's Response to Foreign Extraterritorial Legislation' (2000) 2 Melbourne Journal of International Law, 69, 72.

Shehu, I, M, and Jahun, A, S, Constitutions Making, Amendments, Reviews and Nigeria's Political Development: The Political Economy and Unending Search' (2018) < https://www.academia.edu/36504422/Constitutions_Making_Amendments_Reviews_and_Nigeria_s_Political_Development_The_Political_Economy_and_Un_ending_Search> accessed 30 March 2021.

Sheridan, W and Riley, T 'Comparing E–Government vs E–Governance; (eGov Monitor. Knowledge Asset Management Limited, London, 2006).

Simitis, S, 'From the Market to the Polis: The EU Data Protection Directive on the Protection of Personal Data? (1995) 80 (3) Iowa Law Review, 445–469.

Simitis, S, 'Privacy–An Endless Debate?' (2010) 98(6) California Law Review, 1989, 1995.

Simitis, S, Bundesdatenschutzgesetz, (7th edn (in German), Nomos, 2011) 1.

Singh, U 'E–Governance Implementation–A Literature Review Analysis' (2019) 6(1) IJRAR, 459.

Sixsmith, J, 'House and Home in Old Age' (1985) Paper Presented at British Society of Gerontology Conference, Keele Univeristy.

Sixsmith, J, 'The Meaning of Home: An Explanatory Study of Environmental Experience' (1986) 6 Journal of Environmental Experience 281–298.

Sjaak van der Geest 'Privacy from an Anthropological Perspective 'in the Handbook of Privacy Studies' (Amsterdam University Press, 2018)

Sloan, H, R and Richard Warner, Relational Privacy: Surveillance, Common Knowledge and Coordination (2017) 11(1) University of St. Thomas Journal of Law and public Policy, 7.

Sloot, B 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two–Ticted System' System' (2015) 31 Computer & Security Review, 26, 40.

Smet, S, Freedom of Expression and the Right to Reputation: Human Rights in Conflict (2010) 26 Am. U. Int'l Rev., 183, 184.

Smith, J, Sandra J. Milberg and Sandra J. Burke, 'Information Privacy: Measuring Individual's Concerns About Organisational

Practices' (1996) 20(2) MIS Quarterly, 167.

Solove, D, Understanding Privacy, Harvard University Press, 2008) 5.

Solove, J, D 'A Brief History of Information Privacy Law' in Proskaver on Privacy (PLI, 2006).

Solove, J, D, A Taxonomy of Privacy (2006) 154 (3) University of Pennsylvania Law Review, 477, 564.

Solove, J, D, Understanding Privacy (Harvard University Press, 2008).

Stanlely v Georgia.

Stark, L, The Emotional Context of Information Privacy (2016) 32(1) The Information Society, 16; Andrew Mcstay, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) Big Data & Society 1–12

Stefan Kulk and Frederik Zuiderreen Borgesius 'Privacy of Expression and Right to be Forgotten in Europe' (2017) in Cambridge Handbook of Consumer Privacy (Cambridge University Press, 2018) 1.

Steiner, J, H, and Alston, P, International Human Rights in Context, Law Politics, Morals' (2nd ed Oxford University Press, 2000) 1; Hannum, H, The UDHR in National and international Law (1998) 3(2) Health and Human Rights, 149.

Stephanov, I, 'Introducing a Property Right Over Data in the EU: The Data Producer's Right–An Evaluation' (2019) 34(1)

International Review Law, Computers and Technology, 65.

Stigler G, An Introduction to Privacy in Economics and Politics (1980) 9(4) The Journal of Legal Studies, 623–644.

Stoddart, J, Chan, B and Joly, Y 'The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research, (2016) 44(1) The Journal of Law Medicine and Ethics, 1;

Strahilevitz, J, L, Reunifying Privacy Law (2010) 98(6) California Law Review, 2007–2048.

Strehilevitz, L, 'Privacy Versus Anti–discrimination' (2008) 75 University of Chicago Law Review, 363.

Strobl, J, Cave, E and Walley, T 'Data Protection Legislative: Interpretation and Barriers to Research' (2000) 321(7265) BMJ, 890–892.

Stuart, A, Arosha, K, Bandara and Levine, M, 'The Psychology of Privacy in the Digital Age' (2019) 13 (6) Social and Personality Psychology Compass, 1.

Sun, Y, Zhu, J, Xiong, Y, and Zhu, G, 'Data Security and Privacy in Cloud Computing' (2014) 2014 International Journal of Distributed Sensor Networks, 9.

Sundareswaran, V, Study of Cybersecurity and Data Breaching, (2018) < https://www.researchgate.net/publication/325300571_STUDY_OF_CYBERSECURITY_IN_DATA_BREACHING > accessed 20 June 2021.

Svantesson, DJB, 'Extraterritoriality and Targeting in EU Data

Privacy Law: The Weak Spot' Undermining the Regulation' (2015) International Data Privacy Law 5(4), 226

Tavani, H, Informational Privacy Concepts Theories and Controversies in The Handbook of Information and Computer Ethics Kenneth Himma and Herman T. Tavani, (eds) (John Wiley & sons 2008) 131.

Tavani, H, Philosophical Theories of Privacy: Implication for an Adequate Online Privacy Policy (2007) 38(1) Metaphilosophy, 1.

Teresa Scassy, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy (2010) 7(1) Canadian Journal of Law and Technology, 44.

Tergblad, S 'Is there a New Managerial Work? A Comparison with Henry Mintzberg's Classic Study 30 Years Later' (2006) 43 Journal of Management Studies, 143.

Thoma, F 'How Siemens Assess Privacy Impacts' in *Privacy Impact Assessment,* David Wright and Paul De Hert (eds) (Springer, 212) 277.

Thomas Emerson, 'The Right of Privacy and Freedom of the Press' (1979) 14(2) Harvard Civil Rights for Law Reviews, 330.

Thomas McMullan, 'The World's First Hack: The Telegraph and the Invention of Privacy' (2015) < https://www.theguardian.com/technology/2015/jul/15/first–hack–telegraph–invention–privacy–gchq–nsa> accessed 1 July 2021.

Toom, K, & Pamela F. Miller, 'Ethics and Integrity in Research Management, Europe and Beyond, Jan Andersen, Kristel Toom,

Pamela F. Miller (eds) (Academic Press, 2017) 263–287.

Toom, K, Miller, F, P 'Ethic & Integrity' in Research Management. Europe & Beyond, Jan Andersen, Kristel Toom & Pamela F. Miller (eds) (Academic Press, 2017) 263–287.

Torra, V, Data Privacy: foundations, New Developments and the Big Data Challenge (Spring 2017)

Tovi, D, M and Muthama, N, M 'Addressing the Challenges of Data Protection in Developing Countries' (2013) 1(1) European Journal of jComputer Science and Information Technology, 1–9.

Turner et al, S 'The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IOT) Environment' (2020) New Media of Security, 1–21.

Tzanou, M, 'Data Protection as a fundamental Right Next to Privacy? (2013) 3(2) International Data Privacy Law, 88–99.

Tzanou, M, The Fundamental Right to Data Protection Normative Value in the Context of Counter–Terrorism Surveillance (Hart Publishing, 2017) 12.

Ursic, H 'Unfolding the New Born Right to Data Portability: Four Gateways to Data Subject Control' (2018) 15(1) Journal of Law, Technology &Society, 42–69.

Ustaran, E, European Data Protection Law and Practice (IAPP, 2019) 282.

Uteck, A, Ubiquitous Computing and Spartial Privacy in Lessons from the Identity Trial: Anonymity, Privacy and Identity in a

Networked Society Ian Kerr, Valerie Steeves, Carole Lucock (eds) (Oxford University Press, 2009) 83–102.

Vedaschi, A, and VLubello, "Data Retention and its Implications for the Fundamental Right to Privacy. A European Perspective' (2015) 20 Tilburg Law Review, 14–34.

Veeningen, M, Benne de Weger and Zannone, N, 'Data Minimization in Communication Protocols: A Formal Analysis Framework and Application to Identity Management' (2014) 13 International Journal of Information security, 529–569.

Venkataramanan, N, Data Privacy. Prinicples and Practice (CRC Press 2016)

Ventrella, E 'Privacy in Emergency Circumstances; Data Protection and the COVID–19 Pandemic' (2020) 21 ERA Forum, 379–393.

Voigt P, EU General Data Protection Regulation GDPR: A Practical Guide (Springer International Publishing, 2017) 87.

Voigt, P and Bussche, A, The EU General Data Protection Regulation (GDPR): A Poetical Guide (Springer International Publishing, 2017) 88.

Voigt, P EU General Data Protection Regulation GDPR: A Practical Guide (Springer International Publishing, 2017) 87.

Wacks, R, The Protection of Privacy (Sweet & Maxwell, London, 1980).

Walker, R. 'The English Law of Privacy–An Evelong Human Right' < https://www.supremecourt.uk/docs/speech_100825.

pdf> accessed 14 March 2021.

Walton, S and Marucheck, S, A 'The Relationship Between EDI and supplier Reliability? (1997) 33(3) Information Journal of Purchasing and Material Management 30–35.

Wang, M and Jiang, Z 'The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World' (2017) 11 International Journal of Communication, 3286–3305.

Warren, S and Brandies, L, The Right to Privacy (1890) 4 Harvard Law Review 193. They advocated for the remedy of an action in tort for damages

Warren, S, and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review, 11.

Westin, A, Privacy and Freedom (New York Athenum, 1967) 48.

Whitman, J, The Two Western Culture of Privacy: Dignity Versus Liberty (2004) 77 The Yale Law Journal, 475

Wilkins, G, R, Defining the Reasonable Expectations of Privacy: An Emerging Tripatrite Analysis (1987) 5(5) Vanderbilt Law Review, 1079.

William A. Parent 'A New Definition of Privacy for the Law' (1983) 2(3) Law and Philosophy 305–338

Williams J. Winslade and Judith Wilson Ross, 'Privacy, Confidentiality, and Autonomy in Psychotherapy' (1985) 64(4)

Nebraska Law Review, 580, 582.

Winslade, J, W, and Ross, J, Privacy Confidential and Autonomy in Psychotherapy (1985) 64 (4) Nebraska Law Review, 580.

Wolters, PTJ, 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?' (2017) 7(3) International Data Privacy Law, 165

Wong, J and Henderson, T 'The Right to Data Portability in Practice: Explaining the Implications of the Technology Neutral GDPR' (2019) 9(3) International Data Privacy Law, 173, 174

Wong, R 'Social Networking: The Application of the Data Protection Framework Revisited' (2014)2(2) Birkbeck Law Review, 317–348.

Xanthoulis, E, N 'Negotiating the EU Data Protection Reform: Reflection in the Household Exemption' (2014) Proceedings of the 5th Conference on E–Democracy–Security, Privacy and Trust in a Digital World, Springer CCIS series, vol. 441, 4.

Yann, Pandova, 'Is the Right to be Forgotten a Universal, Regional or 'Global' Right?' (2019) 9(10) International Data Privacy Law, 15.

Yeager, B, M 'Search, Seizure and Positive Law: Expectations of Privacy Outside the Fourth Amendment' (1993) 84(2) Journal of Criminal Law and Criminology, 249.

Yi–Fu Tuan, 'Place. An Existential Perspective (1975) LXV The Geographical Review, 151–165.

Yochai Benkler, 'Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of

Private Rights in Information' (1999) 15 Berkeley Tech Law Journal, 1.

Yusuff, I, 'A Critical Review of the Computer Security and Critical Information Infrastructure Protection Bill 2005 as Nigerian Specific Cybercrime Legislation' (2015) < https://martinslibrary.blogspot.com/2015/03/a–critical–review–of–computer–security.html> accessed 9 March 2021.

Z v Finland, no. 2209/93 ECHR 1997, Digital Rights Ireland and Sertilinger, C. 293/12 and C. 594/12;

Zimmerman, D, False Light Invasion of Privacy: The Light that Failed (1989) 64 New York University Law Review, 375–83

The book is Nigeria's first academic text book on right to privacy and data protection law in Nigeria. It is divided into six parts but sub-divided into 22 chapters to wit: definition of privacy, taxonomy and typology of privacy, right to privacy in Nigeria, privacy as a tort, privacy as a fundamental right, evolution of data protection in Nigeria, sources of data protection law in Nigeria, relationship between data protection and other rights, scope and application of the NDPR, definitions, principles of data protection, lawful bases for data processing, derogation and exemptions, processing of sensitive personal data, data security, rights of data subjects, data protection authority, the enforcement of data protection administrative fines and damages, international transfers of data, personal data breach and suggested reforms.

Olumide Babalola is a prolific and consummate digital rights, consumer rights, privacy and data protection lawyer in Nigeria. He has five published books to his credit: the first is a historical piece on the office of the Attorney General of the Federation and its occupants in Nigeria; the second being a casebook on labour and employment law; the third is another casebook on corporate law and practice; Babalola's Law Dictionary, is reputed as Nigeria's first law dictionary (strictly so called) and his penultimate publication is the Casebook on Data Protection. Olumide is the managing partner of Olumide Babalola, LP - his flagship full service law office with particular bias for digital rights, consumer rights litigation, class actions, employment and corporate commercial litigation et al.

9 789789 964598