DECONSTRUCTING NIGERIA'S DATA PROTECTION REGIME FROM CONSUMER PROTECTION PERSPECTIVE

Submitted: 30 May 2020
Revised: 08 July 2020
Accepted: 13 July 2020

Article submitted to peer blind review

Dike Justin Ibegbulem[*]
ORCID: https://orcid.org/0000-0003-3043-4080
Festus Okechukwu Ukwueze[**]
ORCID: http://orcid.org/0000-0003-0293-5021

DOI: https://doi.org/10.26512/lstr.v13i1.31850

Abstract

Purpose – The purpose of this paper is to make a case for the recognition of privacy and personal data protection as species of consumer rights in Nigeria in line with the revised United Nations Guidelines for Consumer Protection (UNGCP) by amending existing laws or enacting a new law to provide for personal data protection regime for consumers.

Methodology/Approach/Design – The study follows a structured review of relevant extant legislation on consumer protection and personal data protection, namely the Federal Competition and Consumer Protection Act 2018 (FCCPA) and the Nigeria Data Protection Regulation 2019 (NDPR).

Findings – The paper identifies that the provisions of Nigeria's foremost consumer protection legislation, FCCPA, does cover electronic commerce (e-commerce) or consumer privacy and personal data protection while the NDPR, subsidiary legislation on personal data protection, which is yet to be effectively implemented is too general as to provide the consumers the much-needed privacy protection in their dealings with businesses.

Practical Implications–Given the importance Recognition of data privacy and personal data protection as a species of consumer rights helps in understanding consumer protection in online transactions and opens opportunities for future research on consumer privacy and data protection.

Originality/Value – Given the importance attached to the protection of consumer privacy and the various ramifications of transactions involving exposure of consumers' personal data, recognition of privacy consumers' rights to privacy is vital in consolidating knowledge of consumer rights and identifying paths for future research.

[*]LL.M, PhD(C) in the Department of Commercial and Corporate Law, Faculty of Law, University of Nigeria. His research interests include Maritime Law, International Commercial Arbitration, Maritime Arbitration, Alternative Dispute Resolution, Consumer Protection, Cyber-law, and ICT Law. Contact: dike.ibegbulem.pg03576@unn.edu.ng.
[**]Ph.D, Senior Lecturer and currently Head, Department of Commercial and Corporate Law, Faculty of Law, University of Nigeria. He is barrister and solicitor of the Supreme Court of Nigeria. He teaches Law of Consumer Protection, Competition Law, Electronic Commerce Law and Law of Tort. Contact: festus.ukwueze@unn.edu.ng.

Keywords: Consumer Privacy. Personal Data Protection. Consumer Protection. E-Commerce Regulation.

INTRODUCTION

The principal aim of consumer protection is to safeguard the interests of the consumer in their relationships with businesses. Thus, the term consumer protection is generally used to classify measures that ensure that consumers are fairly treated and that their rights are protected in commercial transactions that involve the supply of goods or services.[1]To this end, the United Nations General Assembly adopted the Guidelines for Consumer Protection[2] which sets out the general principles on which the basic rights and legitimate needs of the consumers are centered.[3] These rights and needs include protection for consumers dealing with organizations online and offline and the protection of consumer privacy in the global free flow of information.

Ukwueze posits that the goal of the law in consumer protection is to prevent harm and injury to the consumer, as well as to provide redress for the consumer where he or she suffers harm or injury in his or her relationship with the producer or supplier of goods and services.[4] In the information or computer age, the ultimate goal in these regards is to build "a digital age consumers can trust".[5] Thus, right to personal data protection is indeed a class of consumer rights that is not just cognizable but also enforceable under the law of consumer protection in today's digital age where digital technology especially information and communication technology (ICT) now provides the cheapest and fastest means of conducting commercial transactions via the Internet.[6] Buying and selling

[1]Felicia Monye, *Law of Consumer Protection* (Ibadan: Spectrum, 2013) 19.
[2] United Nations Conference on Trade and Development (UNCTAD, 2016), "United Nations Guidelines for Consumer Protection", United Nations, Geneva, available at: https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf.
[3] Consumers International "Consumer Protection: Why It Matters to You - A Practical Guide to the United Nations Guidelines for Consumer Protection" (London: Consumers International, 2016), https://www.consumersinternational.org/media/2049/un-consumer-protection-guidelines-english.pdf.
[4] F. O. Ukwueze, "Towards a New Consumer Rights Paradigm: Elevating Consumer Rights to Human Rights in South Africa" [2016](32)(2)*South African Journal on Human Rights* 248−271; DOI: 10.1080/02587203.2016.1215655.
[5] Felicia Monye, "Protecting Consumers of Products and Services in the Digital Age" News Commentary to mark the World Consumer Rights Day 2017 (15 March 2017) http://www.consumerawarenessng.org/events/protecting-consumers-of-products-and-services-in-the-digital-age.html.
[6]M. Nuruddeen, Y. Yusof, and A. Abdulla; "Legal Framework for E-Commerce Transactions and Consumer Protection: A Comparative Study" (2015), https://www.researchgate.net/publication/315730418_Legal_Framework_for_Ecommerce_Transactions_and_Consumer_Protection_A_Comparative_Study.

on the Internet otherwise called electronic commerce, is rapidly growing around the globe.[7] The rise in the volume and varieties of online transactions has brought the issue of protection of personal data to the front burner.

Presently, in Nigeria, there appears to be a hodgepodge of instruments regulating personal data protection on electronic commerce platforms. The Nigerian Constitution[8] guarantees the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications. However, apart from this broad constitutional provision, until fairly recently, no law comprehensively set out guidelines for the protection of the privacy of individuals in Nigeria, rather there were a few industry-specific and targeted laws and regulations that provide some privacy-related protections.[9] These include the Cybercrimes Act 2015, which prevents the interception of electronic communications and imposes data retention requirements on financial institutions; the Consumer Code of Practice Regulation 2007 (CCPR), which requires telecommunication operators to take reasonable steps to protect customer information from accidental disclosure and also restricts the transfer of customer information; and the Consumer Protection Framework 2016 (CPF) issued by the Central Bank of Nigeria (CBN), which contains provisions that restrain financial institutions from disclosing the personal information of their customers. There are other pieces of legislation that contain provisions that touch on the protection of privacy rights, such as the Child Rights Act 2003,[10]which reiterates the constitutional right to privacy as it relates to children, and the Freedom of Information Act 2011,[11]which enables public access to public records and information and prevents a public institution from disclosing personal information to the public unless the individual involved consents to the disclosure. Meanwhile, it is noteworthy to mention that, at the regional and continental levels, the Economic Community of West African States (ECOWAS) Data Protection Act 2010[12] and the African Union Convention on Cybersecurity and Data Protection 2014[13] both seek, among others things, to provide a common framework for data protection among member states, including Nigeria. Unfortunately at the time of

[7] C. Omar and T. Anas, "E-Commerce in Malaysia: Development, Implementation and Challenges" [2014](3)(1) *International Review of Management and Business Research*291–298.
[8] Constitution of the Federal Republic of Nigeria 1999 (as amended), section 37.
[9]U. Udoma and B. Osagie, "Data Privacy Protection in Nigeria" (2019)https://www.uubo.org/media/1337/data-privacy-protection-in-nigeria.pdf.
[10] Child Rights Act, No. 26 of 2003, sections 8 and 205.
[11] Freedom of Information Act, No. 4 of 2011.
[12] Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (16 February 2010).
[13]Adopted by the 23rd Ordinary Session of the Assembly, Malabo, Equatorial Guinea (27 June 2014).

writing, neither of these two instruments is operational in Nigeria, having not been domesticated by enactments of the Nigerian legislature as required under Section 12 of the Nigerian Constitution. At the national level, the Electronic Communications and Transactions Bill, modeled after the United Nations Commission on International Trade Law (UNCITRAL) Model Law on E-Commerce, is yet to be passed into law by the Nigerian legislature.[14] The Bill aims to facilitate e-commerce and provides equal treatment to paper and electronic information in trade.

The above situation prompted arguments in academic circles as to whether a personal data protection regime existed in Nigeria. Udoma and Osagie[15]opined that what existed could not be referred to as a personal data protection regime, while Aderibigbe[16] maintained that the pieces of legislation in existence constituted Nigeria's personal data protection regime. Nevertheless, the absence of a principal legal instrument comprehensively regulating personal data protection in Nigeria was quite obvious. This constituted a major source of worry for consumers over the safety of their personal data and privacy on various e-commerce platforms.

In a bid to better protect the interest of consumers, the Nigerian government in January 2019 enacted the Federal Competition and Consumer Protection Act 2018 (FCCPA),[17]whose principal objectives include protecting and promoting the interest and welfare of consumers. Also in a bid to create a general regulatory framework for personal data protection in Nigeria, the National Information Technology Development Agency (NITDA) in January 2019 issued the Nigeria Data Protection Regulation 2019 (NDPR). This paper interrogates the new consumer protection and data protection regimes and questions whether they adequately address the personal data protection concerns of consumers in Nigeria, especially e-commerce aficionados. The paper is structured into five sections with this introduction as the first section. The second section is a discussion of the need for protection of consumer's personal data, while the third and fourth sections review Nigeria's new consumer and data protection regimes. The third section is a synoptic review of the new FCCPA to identify whether and to what extent it recognizes and provides for the protection of consumers' personal data while the

[14]National Assembly "Senate Moves to Legalize Electronic Transactions, Criminalize Online Fraud" (2020), https://www.nassnig.org/news/item/1408; A. S. Aliyu and F. O. Adebayo "Analysis of Electronic Transactions Bill in Nigeria: Issues and Prospects" [2014] 5 (2), *Mediterranean Journal of Social Sciences*, 215 – 220.
[15]Udoma and Osagie (n 9).
[16] See N. Aderibigbe"Nigeria Has a Data Protection Regime" (2017), http://www.jacksonettiandedu.com/nigeria-has-a-data-protection-regime/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.
[17] Federal Competition and Consumer Protection Act, No. 1 of 2019.

fourth section reviews the provisions of the NDPR to ascertain the level of protection it provides for the consumer in online transactions. Lastly, the fifth section, which is the coda, puts forward some prognosis to consumer data protection concerns in Nigeria and generally concludes the paper.

NEED FOR PROTECTION OF CONSUMERS' PERSONAL DATA

All around the globe, an unimaginable number of people carry out different transactions online. Electronic commerce (e-commerce) provides the fastest means for the conduct of commercial transactions within and across national boundaries. It has become increasingly easier for consumers to access a wide range of products and services online. Since the turn of the century, there has been a steady rise in e-commerce, which is expected to rise as mobile Internet and devices such as smartphones, tablets and e-readers become more widespread.[18] Online transactions are proving to have the advantage of being easy, convenient, cheap, and efficient for sellers and buyers. A major benefit of e-commerce is the ability to reach an inestimable audience. Consumers all over the world can view and patronize goods displayed on the Internet, which has the advantage of exposing consumers to a wide range of products helping them to make rational choices without having to spend valuable time travelling to find the goods they need. It helps suppliers of products and services to reach an unimaginable number of consumers around the world.[19] More often than not, payments in online transactions are done electronically and not by physical cash transfer. This has increased the volume of non-cash transactions. It is predicted that the number of non-cash transactions will increase from 538.6 billion in 2017 to 779.2 billion in 2020 with the number of transactions in developing regions increasing from 188.6 billion in 2017 to 350 billion in 2020.[20]

Internet payments and online transactions generally, usually involve the collection and storage of individuals' personally identifiable information (PII) on trading and other platforms of businesses and establishments. Such PII that can be collected and stored include names, aliases, occupation, religious belief and affiliations, telephone numbers, bank accounts details, family information, biometric data, and so on, some of which can be used alone or in combination

[18] See OECD, "Empowering and Protecting Consumers in the Internet Economy", OECD Digital Economy Papers, No. 216 (OECD Publishing, 2013) https://dx.doi.org/10.1787/5k4c6tbcvvq2-en.

[19] F. N. Monye, "Consumer Protection in Electronic Commerce" [2010-2011] 6 *Consumer Journal*, 23.

[20] Capgemini Research Institute "World Payment Report 2019" (2019), https://www.capgemini.com/es-es/wp-content/uploads/sites/16/2019/09/World-Payments-Report-WPR-2019.pdf.

with others to identify the individual concerned.Other unique identifiers include Internet Protocol (IP) address, Media Access Control (MAC) address, International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, Integrated Circuit Card Identifier (ICCID) or Subscriber Identity Module (SIM) and so on, all of which can be used to identify a specific individual. Sometimes personal data of consumers are collected beyond the requirements of particular transactions thereby increasing their vulnerability to the vagaries of internet hackers, fraudsters, and data thieves.[21]Online transactions provide opportunities and avenues for intrusion into the privacy of individual's personal information. The ease with which sensitive information can be intercepted by unauthorized persons has become a major cause of concern. It has been strongly suggested that individuals should have unfavourable perceptions of online shopping security and be wary of giving sensitive information such as credit card details over the Internet.[22]However, excessive apprehension in this regard may cause people to avoid online transactions and thereby lose the advantages and opportunities they provide.

Protection of data privacy has become a topical issue prompting nations to develop and implement data protection legislation aimed at regulating the collection, storage, use, and circulation of personal data. Similarly, until fairly recently, not much attention has been paid to the personal data protection rights of consumers in Nigeria. For example, in 2014, a study on the state of consumer protection in the telecommunications sector in Nigeria omitted entirely reference to personal data protection rights of e-commerce users.[23]Incidentally, in 2015, a review of the United Nations Guidelines for Consumer Protection (UNGCP) was prompted by new issues of consumer concern, generated by extant technology.[24] The revised Guidelines that emerged stipulate that the legitimate needs of the

[21] M. Nuruddeen, "An Appraisal of the Legal Requirements of Electronic Commerce Transactions in Nigeria" [2011] (3)(1) *Bayero University Journal of Public Law*164–183.
[22]J. M. Jones and L. R. Vijayasaratgy, "Internet Consumer Catalog Shopping: Findings from an Exploratory Study and Directions for Future Research" [1998](8)(4)*Internet Research: Electronic Networking Applications and Policy,* 322 – 330; M. Bourlakis, S. Papagiannidis and H. Fox, "E-Consumer Behaviour: Past, Present and Future Trajectories of an Evolving Retail Revolution" [2008](4)(3) *International Journal of E-Business Research*, 64−76.
[23]See Consumers International, "Research Report on the State of Consumer Protection in Nigeria: A Review of Consumer Protection in the Telecommunications Sector in Nigeria" (2014) http://www.consumersinternational.org/media/2255/consumer-protection-in-nigeria-research-report-eng.pdf.
[24] The United Nations Guidelines for Consumer Protection (UNGCP) are a valuable set of principles for effective consumer protection legislation, enforcement institutions and redress systems for assisting interested member States in formulating and enforcing domestic consumer protection laws. First adopted by the UN General Assembly in resolution 39/248 of 16 April 1985, the guidelines were recently revised by the General Assembly in resolution 70/186 of 22 December 2015.

consumer that should be met in consumer protection regulations include,*inter alia*, the provision of a level of protection for consumers using electronic commerce that is not less than that afforded in other forms of commerce; and "the protection of consumer privacy and the global free flow of information".[25]

A recent research report by Consumers International and Internet Society (2019)[26]explored consumer perceptions and attitudes towards trust, security, and consumer privacy concerning the Internet of Things (IoT).. The report shows that connected devices are everywhere but concerns about privacy and security remain limited and that people across markets distrust their connected devices to protect their privacy and handle their information in a respectful manner. The report also indicates that people have reason to believe that their data were being used by other organizations without their permission. At last, it concludes that a high number of people believe that privacy and security standards should be assured by regulators, device manufacturers, and retailers.[27]

In 2017, a review of the data collection practices, policies, and regulations in Nigeria showed that there are five primary concerns around the collection and use of personal data in the country.[28] The findings from the review shows, among other things, that:

(a) the use of personal data may be incompatible with the purpose for which it was collected;
(b) individuals have no rights in relation to the collection, use, and storage of their personal information;
(c) Nigerians are not offered adequate opportunities to consent to or opt-out of data collection;
(d) there is limited-to-no transparency around the processing of personal data, and there is limited information available around how this personal data is used and stored, leading to greater risk of personal data breach; and
(e) children are exposed to privacy risks online and often lack the legal capacity to give valid consent, and may unknowingly disclose personal information to online platforms due to the appealing nature of their visual content.

[25] UNGCP Article III Rule 5 Paras (j) and (k).
[26] Consumers International and the Internet Society (2019) "The Trust Opportunity: Exploring Consumer attitudes to the Internet of Things" (2019) https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/.
[27] Ibid.
[28]World Wide Web Foundation (2018) "Personal Data Protection in Nigeria" (2018): http://www.webfoundation.org/docs/2018/03/WF_Nigeria_Full-Report_Screen_AW.pdf.

These have heightened the need for data protection regulation in Nigeria which should take cognizance of and give due attention to the protection of consumers' personal data in their dealings with undertakings.

CONSUMER DATA PROTECTION UNDER FCCPA 2018

On 30 January 2019, Nigeria's president, Muhammadu Buhari signed into law the Federal Competition and Consumer Protection Bill earlier passed by the National Assembly in 2018.The key objectives of the legislation, known as the Federal Competition and Consumer Protection Act 2018 (FCCPA), are to promote and maintain competitive markets in the Nigerian economy; promote economic efficiency; protect and promote the interests and welfare of consumers by providing consumers with a wider variety of quality products at competitive prices; prohibit restrictive or unfair business practices which prevent, restrict or distort competition or constitute an abuse of a dominant position of market power in Nigeria; and contribute to the sustainable development of the Nigerian economy. The Act applies to all commercial activities undertaken for profit and satisfaction of public demand in the country. This is regardless of whether these activities are undertaken by private or public entities or agencies of the federal, state, or local government. It repealed the Consumer Protection Council (CPC) Act 1992 and established a new commission known as the Federal Competition and Consumer Protection Commission ("FCCPC" or "the Commission") and transferred assets, liabilities, and employees of the erstwhile Consumer Protection Council (CPC) established under the former law to the Commission.[29] By Section 104 of FCCPA, the provisions of the Act override the provisions of other laws in all matters relating to competition and consumer protection, subject only to the provisions of the Nigerian Constitution.[30]

As privacy protection is now recognized as a legitimate consumer need, some pertinent questions arise.[31]First, how does Nigeria's new consumer protection legislation provide for the protection of the personal data of consumers? Put differently, does FCCPA guarantee protection of personal data and security for consumers in line with the revised UNGCP? A related question is, whether FCCPC is adequately equipped and competent to handle the protection of consumers' data by undertakings that are subject to FCCPA?

[29]FCCPA, Section 166 and the Second Schedule.
[30] Ibid, Sections 1, 2 and 104
[31] See T. Ndunagu "Nigeria's Journey to Richland: Turning things up a notch with the Federal Competition and Consumer Protection Act" (2019), https://infusionlawyers.com/nigerias-journey-to-richland-turning-things-up-a-notch-with-the-federal-competition-and-consumer-protection-act/.

The function of FCCPC include administering and enforcing the provisions of FCCPA and any other competition and consumer protection law; eliminating anti-competitive agreements, misleading, unfair, deceptive, or unconscionable marketing, trading, and business practices; and giving and receiving advice from other regulatory authorities or agencies within the relevant industry or sector on consumer protection and competition matters. Its other functions include authorizing, prohibiting, or approving mergers and encouraging trade, industry, and professional associations to develop and enforce in their various fields quality standards designed to safeguard the interest of consumers.[32]

FCCPA recognizes several consumer rights and makes provisions geared towards the protection of those rights. These include rights to:

(a) information, including the right to disclosure of price of goods or services,[33] product labeling, and trade descriptions[34] and transaction records;[35]
(b) choose which covers the right to choose or examine goods,[36]select suppliers,[37] cancel reservation, booking or order[38] and to reject or return unsafe or defective goods;[39]
(c) fair dealings,[40] including the right to general standards for the marketing of goods and services;[41]
(d) safe and quality goods and services;[42]
(e) be heard, including the right of complaint to the supplier of goods and services as well as the Commission;[43] and
(f) redress by the Commission, courts, and civil society groups.[44]

In favour of consumers, FCCPA imposes obligations on manufacturers, importers, distributors, and suppliers of goods and services which among others include duties to label goods properly and to withdraw hazardous goods from the

[32] FCCPA, Sections 9 and 17.
[33]Ibid Section 115.
[34]Ibid Section 116.
[35]Ibid Section 118.
[36]Ibid Section 121.
[37]Ibid Section 119.
[38]Ibid Section 120.
[39]Ibid Section 122
[40]Ibid Section 124
[41]Ibid Section 123
[42]Ibid,Sections 130– 131.
[43]Ibid,Section 148.
[44]Ibid,Section 146 and 151 – 152.

market. It also imposes on the suppliers of goods and services liability for defective and services goods and misrepresentation.[45]

None of the consumer rights recognized and protected in the FCCPA deals with consumer privacy or personal data. The obvious implication of this omission is that consumers' privacy rights are yet to be accorded full recognition as a species of consumer rights under Nigeria's primary consumer protection regime. One is thus left to wonder why the drafters of FCCPA failed to take account of the relevant principles under the extant UNGCP on the protection of consumers using e-commerce and the protection of consumers' privacy. Another remarkable omission in the Act, which ordinarily should be an upgrade of the repealed CPC Act, is the total omission of any reference to and therefore non-regulation of e-commerce. This calls into the question of the purported all-inclusiveness of the Act and by extension, the jurisdiction of FCCPC over e-commerce transactions. It may be argued that, since the Commission has concurrent jurisdictions with other agencies or relevant authorities in matters of competition and consumer protection (Section 105), inferentially its jurisdiction covers consumer's privacy and data protection as contained in the laws establishing those other agencies and authorities. For example, in the information technology sector, the Commission now has concurrent jurisdiction with the National Information Technology Development Agency (NITDA). Similarly, in the communications sector, the Commission now has contemporaneous jurisdiction with the Nigerian Communications Commission (NCC). Likewise, in the financial sector, the Commission is vested with parallel jurisdiction with the Central Bank of Nigeria (CBN), regardless of CBN's already existing Consumer Protection Framework.

To carry out its tasks efficiently and effectively, the Commission is required to collaborate with other regulatory authorities, trade, industry, and professional organizations locally and internationally. These collaborations will necessarily involve Ministries, Departments and Agencies of the federal government, especially regulatory bodies such as NITDA, NCC, CBN, Standards Organisation of Nigeria (SON), National Agency for Food Drugs Administration and Control (NAFDAC), Securities and Exchange Commission (SEC), and others involved in competition and consumer protection, as well as related matters. However, to avoid possible regulatory frictions with other regulatory authorities, that FCCPA in Section 104 provides that the Act is superior to all other laws in Nigeria, apart from the Constitution. Thus, the Commission's powers take precedence over and above the powers of other relevant government agencies. This provision for coordinate jurisdiction with other agencies in the Act, as some have rightly submitted, "literally kicks things up a notch".[46] For instance, while it

[45]FCCPA Part XVI, Sections 134 – 140.
[46]Ndunagu (n 31).

is a noble idea to have a unified competition and consumer protection regulation, having such law governing the affairs of all sectors, including sectors already regulated, is not quite practicable. This creates room for friction in terms of regulatory roles. For example, if FCCPA had made provisions for privacy and data protection of consumers, invariably there will be a conflict with the role NITDA in data protection and privacy of data subjects. FCCPA's precedence over sector specific regulations may result in inefficiency and consequently defeat the objectives of the Act. The superiority of the Act over other relevant laws and regulations in Nigeria, particularly those concerning consumer protection, might lead to undesired consequences. The same goes for the provision under Section 104(4) of FCCPA where negotiation is stipulated as the primary mode of resolving any impasse that might arise between the Commission and relevant regulatory agencies, which puts the Commission in a superior position, as it will always prevail in such negotiations. Consequently, there is need for some level of deference on the Commission's part and recognition of the capabilities, experience, expertise, and technical knowledge of the relevant regulatory agencies, otherwise, the level of harmonization the Act requires and contemplates will be difficult to attain.

In some other African countries like Ghana and South Africa, as well as in some Association of Southeast Asian Nations (ASEAN) like Singapore, separate data protection legislation has been put in place to address the privacy concerns of data subjects. For instance, the Ghana Data Protection Act 2012,[47]the South African Protection of Personal Information Act 2013[48], and Singapore's Personal Data Protection Act,[49] each recognizes and protects personal data of data subjects. The Malaysian Consumer Protection Act 1999 (as amended)[50]specifically provides for the protection of consumers in online transactions. Under the Act, unfair trade practices in online shopping are defined to include deceptive advertising techniques such as "bait and switch". Furthermore, in the Consumer Protection (Amendment) Act 2010, a new Part 111A, which deals with unfair contract terms has been inserted into the Act. Under this provision, consumers may challenge the validity of standard terms of online contracts for being either procedurally or substantively unfair. Most importantly, consumers who are dissatisfied with online dealings can file their claims in the Tribunal for Consumer Claims which was set up to provide speedy, inexpensive, and informal redress of consumers' grievances.

[47]Data Protection Act 2012.
[48]Protection of Personal Information Act No. 4 of 2013.
[49]Personal Data Protection Act 2012.
[50] Malaysian Consumer Protection Act 1999

There is no equivalent recognition and protection of consumers in online transactions under Nigeria's FCCPA and it is submitted that FCCPC lacks jurisdiction to entertain matters relating to consumer privacy or data protection in online transactions which arise from the breach of the provisions of other statutes which have put in place regulatory bodies for their own enforcement.

CONSUMER DATA PROTECTION UNDER NDPR 2019

On 25 January 2019, NTIDA issued the Nigeria Data Protection Regulation (NDPR), the stated objectives of which include: safeguarding the rights of natural persons to data privacy; fostering safe-conduct for transactions involving the exchange of personal data; preventing manipulation of personal data; and ensuring that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection that is in tune with best practices.

NDPR applies to all transactions involving the processing of personal data notwithstanding how the data processing is conducted, and to all natural persons resident in the country as well as Nigerians residing abroad. The extension of the application of the regulation to the protection of personal data of Nigerian citizens residing outside the country's territory raises the question of enforceability. However, the regulation contemplates collaboration with regulatory and law enforcement authorities in other countries in order to, among other things, develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data and the transfer of personal data to a foreign country or an international organization.[51]

Part 1.3 of the regulation defines personal data as any information relating to an identified or identifiable natural person, who is considered a data subject. In this regard, a data subject is someone who can be identified, directly or indirectly, in particular, by reference to an identifier such as a name, an identification number, location, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Within the context of personal data, processing means:

> 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[52]

[51]NDPR Parts 2.11(a) and 4.3(a).
[52] Ibid,Part 1.3 (r).

NDPR classifies a certain category of data as "sensitive personal data". However, apart from identifying this class of personal data, NDPR makes no provision for different standards in treating them as is the case in personal data laws of other jurisdictions which usually accord this class of data special consideration because of their sensitive nature.[53] Such sensitive personal data are "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."[54]

GOVERNING PRINCIPLES OF DATA PROCESSING UNDER NDPR

Part 2.1(1) of NDPR provides that personal data are to be:

(a) collected and processed in accordance with specific, legitimate and lawful purpose consented to by the data subject; provided that:
    i. further processing may be done only for archiving purposes in the public interest, scientific, historical or statistical research purposes; and
    ii. any persons or entity carrying out or purporting to carry out data processing shall not transfer any personal data to any person.
(b) adequate, accurate and without prejudice to the dignity of the human person;
(c) stored only for the period within which it is reasonably needed; and
(d) secured against all foreseeable hazards and breaches such as theft, cyber-attack, viral attack, dissemination, manipulations, or any kind, damage by rain, fire, or exposure to other natural elements.

Anyone entrusted with or in possession of personal data owes a duty of care to the data subject and is accountable for his or her acts or omissions in respect of data processing under the principles contained in the regulation which are highlighted in the following paragraphs.

[53] Templars "Nigeria Data Protection Regulation 2019: A Safety Net for Personal Information or Just Band-Aid?" (25 March 2019) https://www.templars-law.com/nigeria-data-protection-regulation-2019-a-safety-net-for-personal-information-or-just-band-aid/.
[54] NDPR Part 1.3 (xxv). These are similar to the "special categories of personal data" for which special provisions are made in Articles 9 and 10 of EU General Data Protection Regulation (GDPR)54, Section 10 of UK Data Protection Act 2018 (UKDPA), "special personal information" in part B, Sections 26 – 33 of South Africa's Protection of Personal Information Act, 2013 (POPIA) and as "special personal data" in Ghana's Data Protection Act, 2012 (GDPA).

Fair and Lawful Processing of Data

The foremost principle of data processing is that processing of data must be for legitimate purposes and must be fair. Processing of data is lawful if it meets at least one of the conditions set down in Part 2.2 of NDPR, which include the data subject's consent to the processing of his or her personal data for one or more specified purposes such as the performance of a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract. Consequently, processing of personal data in all forms of commercial transactions in which consumers daily engage in, including e-commerce, qualifies as lawful purpose under the regulation. Even, personal data of a consumer collected while window shopping on the Internet will satisfy the requirement of lawful purpose since such a visit to the website of an undertaking is a necessary preliminary to entering into a transaction with the undertaking.

NDPR prohibits improper motives in processing of personal data. Thus, consent for data processing shall not be sought, given or accepted in any circumstance that may directly or indirectly engender propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts (Part 2.4). It however, does to make specific provisions relating to the protection of children who by their nature are deemed to be less aware of the risks, consequences and safeguards involved the processing of their personal data. The standard is to require the consent, of the holder of parental responsibility of a child, for the processing of the personal data of the child and in some cases prohibit the processing of the personal data of a child for certain purposes.

Consent and Objection

Under Part 2.3, personal data shall not be obtained except if the specific purpose of the collection is made known to the data subject and his or her consent is obtained without fraud, coercion, or undue influence. It is for the data controller to demonstrate not only that the data subject consented to the processing of his or her personal data but that he or she possesses the requisite capacity to give consent and was informed of his right as well as the ease to withdraw his consent at any time. The regulation safeguards the right of a data subject to object to the processing of his or her data. In that regard it provides that a data subject shall have the option to object to the processing of personal data relating to him or her which the data controller intends to process for the purposes of marketing and should be expressly and manifestly offered the mechanism to object to any form of data processing free of charge.

Due Diligence

NDPR imposes liability on data processors and controllers for the actions or inactions of third parties engaged by them to handle the personal data of data subjects. Thus, contracts between data controllers and third parties for the

processing of personal data must be in writing and it is the responsibility of the data controller to ensure adherence to the regulation.[55] Data controllers are required to take reasonable measures to ensure that the other party to the data processing contract does not have a record of violating data processing principles set out in the regulation.

Data Privacy and Security

Anyone involved in the control of the processing of personal data is mandated to develop security measures to protect such data. The prescribed measures include, but are not limited to, protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data and other sensitive or confidential data, protecting emailing systems and continuous capacity building for staff.[56] The prescribed security measures appear to be adequate as they cover all conceivable hazards and breach but there is no requirement for responsible parties to regularly confirm the effective implementation of the safeguards and update such safeguards in response to new risks or deficiencies in previously implemented safeguards.

RIGHTS OF DATA SUBJECTS UNDER NDPR

Right to Information

NDPR recognizes and upholds the constitutional right to privacy by the requirement that the exercise of the rights of data subjects under the regulation shall conform with constitutionally guaranteed principles of law for the general protection and enforcement of fundamental rights.[57] Privacy rights shall be interpreted to advance and never to restrict the safeguards a data subject is entitled to under any data protection instrument made in furtherance of fundamental rights and other Nigerian laws.[58]

Data subjects have extensive rights to information relating to the collection, processing, storage, and transfer of their personal data. Any means through which personal data is being collected or processed shall display a simple and conspicuous privacy policy that the class of data subjects being targeted can understand. Such a privacy policy shall contain information such as what constitutes the data subject's consent; a description of collectable personal information; the purpose of collection of personal data; and technical methods used to collect and store personal information, cookies, web tokens, etc. It should

[55]Ibid,Part 2.7.
[56] Ibid, Part 2.6.
[57] Ibid,Part 3.1(16)
[58] Ibid,Part 2.9

also contain information relating to access (if any) of third parties to personal data and purpose of access; a highlight of the data processing principles stated in the regulation; available remedies in the event of a violation of the privacy policy; the time frame for remedy; and any limitation clause. The data controller shall take appropriate measures to provide the data subject any information relating to the processing of data in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. The information shall be in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally.[59]

Where a data subject requests a data controller to take any action relating to the processing of his or her personal data, and the controller does not act on the request, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and the possibility of lodging a complaint with a supervisory authority.[60] The information provided to the data subject and any communication as well as any actions taken shall be free of charge except as provided in the regulation. But where requests from a data subject are manifestly unfounded or excessive, in particular, because of their repetitive character, the controller may either charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested or decline the request in writing to the data subject. In the event of decline, the controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.[61]

Prior to collecting personal data from a data subject, the controller shall provide certain information, which include: the identity and the contact details of the controller and the data protection officer designated by the controller; the purposes of, and legal basis for, processing the personal data; and the recipients or categories of recipients of the personal data, if any. Other pieces of information to be supplied are the period for which the personal data will be stored, or the criteria used to determine that period; the data subject's rights to access, rectify, restrict the use of or erase data as well as his or her right to data portability, withdrawal of consent, and to complaints with the relevant authority.[62]

Right to Have Personal Data Deleted

A data subject has the right to request the controller to delete his or her personal data and the controller shall comply without delay, especially where these data are no longer necessary considering the purposes for which they were

[59]Ibid,Part 3.1(1).
[60]Ibid,Part 3.1(2)
[61]Ibid,Part 3.1(4)
[62]Ibid,Part 3.1(7).

collected or processed. Other grounds on which a data subject's right to request deletion of data include where the data subject withdraws consent on which the processing is based; the data subject objects to the processing and there are no overriding legitimate grounds for the processing; the personal data have been unlawfully processed; or the personal data must be erased for compliance with a legal obligation in Nigeria. In any case, the particular controller who has made the personal data public and is obliged to delete the personal data shall take all reasonable steps to inform other controllers processing the personal data of the data subject's request.[63]

Right to Restrict Processing of Personal Data

A data subject has the right to obtain from the controller restriction in the processing his or her personal data where one of the following conditions apply:

(a) the accuracy of the personal data is contested by the data subject for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; and
(d) the data subject has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.[64]

Where processing has been restricted such personal data shall, except for storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or the protection of the rights of another natural or legal person or reasons of important public interest in Nigeria.[65]

Right to be Notified of Rectification, Erasure or Restriction of Personal Data

The data controller shall communicate any rectification or erasure of personal data or restriction to each recipient to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort. In that

[63] Ibid, Part3.1 (9) and (10).
[64]Ibid, Part 3.1(11).
[65] Ibid, Part 3.1(12).

case, if the data subject requests, the controller shall inform him or her about those recipients.[66]

Right to Receive and Transmit Personal Data

A data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used machine-readable format. A data subject also has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent or contract, and the processing is carried out by automated means.[67]Similarly, in the exercise of the right to data portability, a data subject has the right to have his or her personal data transmitted directly from one controller to another, where this is technically feasible; provided that this right shall not apply when the processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.[68]

It appears that NDPR does not prescribe any mitigating measures that can be adopted on the occurrence of personal data breach. This omission is not peculiar to NDPR but is noticeable in even seemingly extensive data protection laws including the General Data Protection Regulation of the European Union. Although a cardinal aim of data protection laws is the prevention of such breaches, there is need to include in such laws remedial steps to be taken in the event of a breach, since even the most extensive and efficiently enforced data protection laws cannot be foolproof, in light of continuous technological advancement and increasing sophistication of cybercriminals.[69]

PENALTY FOR DEFAULT

NDPR imposes liability on any person who breaches the data privacy rights of any data subject. In addition to any other criminal liability, it imposes fines as follows:

(a) in the case of a data controller dealing with more than 10,000 data subjects, payment of a fine of 2% of the annual gross revenue of the preceding year, or payment of the sum of ₦10 million.
(b) in the case of a data controller dealing with less than 10,000 data subjects, payment of the fine of 1% of the annual gross revenue of the

[66] Ibid, Part 3.1(13).
[67]Ibid, Part 3.1(14).
[68] Ibid Part 3.1 (14) and (15).
[69]Templars (n 53).

preceding year, or payment of the sum of ₦2 million whichever is greater.[70]

Any breach of the regulation shall be construed as a breach of the provisions of the NITDA Act 2007.71Under the Act, any person or corporate body who contravenes or fails to comply with the provisions of the Act commits an offense.[72]Anybody, corporate or individual who commits an offense under the Act where no specific penalty is provided, is liable on conviction to a fine of ₦200,000.00 or imprisonment for a term of 1 year or to both such fine and imprisonment, for a first offense and a fine of ₦500,000.00or to imprisonment for a term of 3 years or to both such fine and imprisonment, for a second and subsequent offense.[73]

ENFORCEMENT AND REDRESS MECHANISMS

Within three months after the date of issuance of NDPR, all public and private organizations in Nigeria that control data of natural persons shall make available to the general public their respective data protection policies which shall be in conformity with the regulation.[74] The three months grace period given to relevant data controllers to comply with the provisions of NDPR is evidently too short to enable them to set up the required data protection mechanisms. Under the GDPR the grace period was two years.[75] For a country that did not have a prior regulation that required the kind of skill and technical capacity envisaged three months only is far too short. Every data controller shall designate a data protection officer for the purpose of ensuring adherence to the regulation, relevant data privacy instruments, and data protection directives of the controller. However, a data controller may outsource data protection to a verifiably competent firm or person.[76] Every data controller or processor shall ensure continuous capacity building for her data protection officers and the generality of her personnel involved in any form of data processing.[77] Without prejudice to the right of a data subject to seek redress in a court of competent jurisdiction, the Agency shall set up an Administrative Redress Panel (ARP) to investigate allegations of any breach of the provisions of the regulation and determine appropriate redress.

---

[70] NDPR Part2.1
[71] Ibid,Part 4.2(6). The import of this also may be that the penalty provisions of Sections of the NITDAAct apply to the contravention of NDPR.
S[72] NITDA Act, Section 17(1).
[73] Ibid,Sections 17 and 18.
[74]NDPR Part 4.1(1)
[75]GDPR Preamble, Para 171.
[76]Ibid,R 4.1(2)
[77]Ibid,R 4.1(3).

Even though only three months grace period was given to data controllers to comply with the provisions of NDPR, its implementation appears to have suffered a serious setback. It was not until 11 July 2019 that NITDA released a draft framework for its implementation.[78] The draft framework focuses on the implementation of the regulation, particularly in the areas of compliance and enforcement. The enforcement process for cases of breach of personal data under the draft framework centers on surveillance, complaint filing, investigation, notice of enforcement, administrative penalties as well as criminal prosecution. When adopted and fully implemented, the framework will likely result in more efficient enforcement of the provisions of the regulation. However, over one year after the publication of the draft, a final version of the framework is yet to be published.

PROGNOSIS AND CONCLUSION

There is no doubt that proper regulation of the e-commerce subsector is crucial to the future of the national and economic development of any country. E-commerce regulation cannot be adequate without consumer privacy or personal data protection mechanisms. Such mechanisms ensure that key players are properly guided; that consumers are assured of the safety of their personal data. In addition, they also assist the government to generate needed revenue to invest in the economy.[79] It is obvious that FCCPA does not address the privacy concerns of Nigerian consumers who engage in e-commerce. In line with the revised UNGCP, personal data protection and the right to privacy should, as of necessity, be recognized as a consumer right. Given the evident shortcomings of the FCCPA in that regard, an amendment of the Act is imperative to cover the regulation of e-commerce and associated privacy issues. Alternatively, separate legislation should be enacted to regulate the rapidly growing e-commerce sector in Nigeria.

In revising or amending FCCPA or enacting an e-commerce law, the Nigerian legislature could borrow from the State of California's most recent Consumer Privacy Act 2018 (effective from January 2020) which contains many innovative provisions, including consumers' right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of third parties with which the information is shared. Additionally, businesses should be mandated to make disclosures about the information and the purposes for

[78]See NITDA, "Nigeria Data Protection Regulation 2019: Draft Implementation Framework" (2019) https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf.
[79] A. A. Oluwatobi, "Legal Issues in Regulating the E-Commerce Sub-sector in Nigeria" https://www.pressreader.com/nigeria/thisday/20160412/281827167926865.

which data is used; offer financial incentives for collection of personal information; and prohibited from selling the personal information unless affirmatively authorized by the data subject. It should also provide for the right of consumers to request the deletion of personal information and prescribe the requirements for receiving, processing, and satisfying these requests from consumers.[80]

In the meantime, there is a need to elevate NDPR, a subsidiary legislation, to the status of a substantive Act of the National Assembly, as is the case in many other jurisdictions just as Singapore and South Africa. Such an enactment can borrow from Singapore's Personal Data Protection Act 2012 and EU's General Data Protection Regulation (GDPR) both of which contain data protection principles consistent with those contained in the African Union Convention on Cyber Security and Personal Data Protection.

Globalization and the Internet have doubtlessly turned the world into a global hamlet and ushered in the present era of e-commerce. In Nigeria as of today, there are still security concerns relating to Internet transactions and personal data safety amongst consumers engaging in e-commerce transactions. This apprehension is heightened by the seemingly fragmented and inadequate legal framework for personal data protection in the country, stemming largely from the delayed passage into law of the Electronic Transactions Bill which has been pending before the National Assembly since 2011. This bill is patterned after the UNCITRAL Model Law on E-Commerce which is designed to facilitate commerce conducted by electronic means and providing equal treatment to paper-based and electronic information in trading.

In conclusion, it has been shown that, under FCCPA, consumer privacy and personal data protection rights are virtually unrecognized as a species of consumer rights. The non-recognition of consumer privacy rights in FCCPA patently goes against the revised UNGCP's recognition of consumers' right to privacy. However, NDPR contains copious provisions on personal data protection which can be applied to consumers. Considering today's Information or Computer Age, there is a need for the construction of a digital scenario in which consumers can trust. It is therefore submitted that to boost trust in the existing regulatory framework, personal data protection should be given due recognition and prominence as a species of consumer rights in Nigeria's consumer protection regime. Thus, it is imperative that the FCCPA should be amended to include consumers' right to privacy. The National Assembly is also urged to enact into law the Electronic Transactions Bill 2011 in order to regulate peculiar aspects of e-commerce in the country. Finally, it is recommended that the NDPR should be

[80]See California Consumer Privacy Act 2018 Legislative Counsel's Digest, https://www.pbwt.com/content/uploads/2018/06/California-Consumer-Privacy-Act1.pdf.

elevated to the status of an Act of Parliament instead of subsidiary legislation and a separate personal data protection commission, distinct from NITDA, should be established for its enforcement.

REFERENCES

ADERIBIGBE, N. Nigeria Has a Data Protection Regime 2019 http://www.jacksonettiandedu.com/nigeria-has-a-data-protection-regime/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original(Access on 20 April 2020)

ALIYU, A. S.; ADEBAYO, F.O., Analysis of Electronic Transactions Bill in Nigeria: Issues and Prospects **Mediterranean Journal of Social Sciences**, v. 5, n. 2, p. 215 – 220, 2014.

BOURLAKIS, M.; PAPAGIANNIDIS, S.; FOX, H. E-consumer Behaviour: Past, Present and Future Trajectories of an Evolving Retail Revolution. **International Journal of E-Business Research**, v. 4, n. 3, p. 64-76, 2008.

CAPGEMINI RESEARCH INSTITUTE World Payment Report 2019 https://www.capgemini.com/es-es/wp-content/uploads/sites/16/2019/09/World-Payments-Report-WPR-2019.pdf (Access on 12 May 2020).

CONSUMERS INTERNATIONAL Research Report on the State of Consumer Protection in Nigeria: A Review of Consumer Protection in the Telecommunications Sector in Nigeria2014http://www.consumersinternational.org/media/2255/consumer-protection-in-nigeria-research-report-eng.pdf(Access on 13 March 2020).

CONSUMERS INTERNATIONAL Consumer Protection: Why it Matters to You - A Practical Guide to the United Nations Guidelines for Consumer Protection 2016https://www.consumersinternational.org/media/2049/un-consumer-protection-guidelines-english.pdf(Acess on21 April 2020).

CONSUMERS INTERNATIONAL; INTERNET SOCIETY. The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things 2019https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/ (Access on14 May 2020).

JONES, J. M.;VIJAYASARATGY, L. R. Internet Consumer Catalog Shopping: Findings from an Exploratory Study and Directions for Future Research

Internet Research: Electronic Networking Applications and Policy v. 8 n. 4, p. 322-330, 1998.

MONYE, F.N. **Law of Consumer Protection**, Ibadan: Spectrum Books 2013.

MONYE, F.N. Consumer Protection in Electronic Commerce **Consumer Journal** v. 6, p. 1-28, 2011.

NATIONAL ASSEMBLYSenate Moves to Legalize Electronic Transactions, Criminalize Online Fraud (27 February 2020) https://www.nassnig.org/news/item/1408(Access on 12 May 2020).

NDUNAGU, T. Nigeria's Journey to Richland: Turning Things up a Notch with the Federal Competition and Consumer Protection Act (2019) https://infusionlawyers.com/nigerias-journey-to-richland-turning-things-up-a-notch-with-the-federal-competition-and-consumer-protection-act/(Access on 23 April 2020).

NITDA **Nigeria Data Protection Regulation 2019: Draft Implementation Framework** (2019) https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf (Access on 5 November 2019).

NURUDDEEN, M. An appraisal of the legal requirements of electronic commerce transactions in Nigeria **Bayero University Journal of Public Law** *v.* 3, n. 1, pp. 164-183, 2011.

NURUDDEEN, M.;YUSOF, Y.;ABDULLA, A. **Legal framework for E-Commerce Transactions and Consumer Protection: A Comparative Study** (2015) https://www.researchgate.net/publication/315730418_Legal_Framework_for_Ecommerce_Transactions_and_Consumer_Protection_A_Comparative_Study (Access on 15 April 2020).

OECD Empowering and Protecting Consumers in the Internet Economy, **OECD Digital Economy Papers, No. 216**, OECD Publishing, 2013. https://dx.doi.org/10.1787/5k4c6tbcvvq2-en.

OMAR, C.; ANAS, T. E-commerce in Malaysia: Development, Implementation and Challenges **International Review of Management and Business Research,** v. 3, n. 1, p. 291-298, 2014.

TEMPLARS**Nigeria Data Protection Regulation 2019: A Safety Net for Personal Information or Just Band-Aid?"** (25 March 2019) https://www.templars-law.com/nigeria-data-protection-regulation-2019-

a-safety-net-for-personal-information-or-just-band-aid/ (Aceess on3 May 2020).

UDOMA, U.;OSAGIE, B. Data Privacy Protection in Nigeria (2019) https://www.uubo.org/media/1337/data-privacy-protection-in-nigeria.pdf (Access on 23 April 2020).

UKWUEZE, F. O. Towards a New Consumer Rights Paradigm: Elevating Consumer Rights to Human Rights in South Africa **South African Journal on Human Rights**, v. 32, n. 2, p. 248-271, DOI: https://doi.org/10.1080/02587203.2016.1215655.

UNCITRAL **Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998** (1998) https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce (Access on21 May 2020).

WORLD WIDE WEB FOUNDATION Personal Data Protection in Nigeria (2018) http://webfoundation.org/docs/2018/03/WF_Nigeria_Full-Report_Screen_AW.pdf (Access on12 May 2020).

Legislation

Nigeria

Child Rights Act 2003
Constitution of the Federal Republic of Nigeria 1999 (as amended)
Consumer Protection Council Act, Cap 25, Law of the Federation of Nigeria (LFN) 2004.
Cybercrimes (Prohibition, Prevention, etc.) Act 2015
Federal Competition and Consumer Protection Act, No. 1 of 2019.
Freedom of Information Act 2011
National Information Technology Development Agency (NITDA) Act 2007
Nigeria Data Protection Regulation 2019 (NDPR) (30 January 2019).

Other Countries

Consumer Privacy Act 2018 (California, USA)
Consumer Protection (Amendment) Act 2010 (Malaysia)
Consumer Protection Act 1999 (Malaysia)
Data Protection Act 2012 (Ghana)
Data Protection Act 2018 (UK)
General Data Protection Regulation (EU)
Personal Data Protection Act 2012 (Singapore)
Protection of Personal Information Act No. 14 of 2013 (South Africa)

International Standards

African Union Convention on Cybersecurity and Data Protection (27 June 2014).

ECOWAS Data Protection Act 2010 (16 February 2010).

UNCITRAL Model Law on Electronic Commerce (1998).

United Nations Guidelines for Consumer Protection, GA Res 70/186 (22 December 2015).