DATA PRIVACY PROTECTION: OVERVIEW OF THE LEGAL FRAMEWORK IN NIGERIA*

Abstract

The privacy of individuals has always been under attack from both the excessive exercise of the right to free speech, and the commercialization of personal data of celebrities (especially) and ordinary people, alike. However, the advent of the internet introduced easy and cheap means of accessing, caching and transmitting data; thus, placing the attacks on privacy rights on steroids. This paper interrogates the available legal frameworks for the protection of the privacy right in Nigeria. It addresses the issues of how extensive and how effective these legal frameworks are in the protection of data privacy in Nigeria. In researching this paper, such, analytical tools as, meta-analytical style doctrinal comparisons, overt and covert interviews, including resort to both primary and secondary sources of law, were deployed. This paper establishes that Nigeria boasts of fairly adequate laws for the protection of the privacy of individuals and groups of individuals, but that there also exist substantive loopholes that need to be plugged through amendments and proactivity, to keep pace with the fast-paced sphere of the internet. It summarizes that the ease of acquiring, storing and disseminating data in the internet era is a clear and present danger to the protection of data privacy. Finally, it thus recommends the plugging of the existing loopholes in the existing legal frameworks for the protection of personal data. It also recommends the maintenance of a relentless vigil to spot new gaps in the existing Nigerian legal frameworks, in order to keep up with developments in the ever dynamic world of the internet.

Keywords: Privacy, Computer, Protection, Legal Frameworks

1. Introduction

In Nigeria, like in most nations of the world, the fact of the existence of personal identifying data in the custody of many public institutions may have placed these data in the public domain, but that does not presuppose that such data are no longer the private and personal (incorporeal) properties of the data subject. There is, thus, a bounden duty on every institutional/ regular data custodian, and, on the random data poacher, to duly respect the rights of the data subject to the privacy of his personal data. A regular and relentless threat to the inviolate protection of this personal data, however, is the fact that data is now a means of isolating potential customers of products and services, for targeted online advertising; hence, the sale of these personal identifying data is a real source of income for online based firms. Most of these data-poaching online firms very readily offer free access to their sites, as bait for data subjects, whose personal identifying data they thus harvest and commercialized. Even firms desirous of protecting their industrial/ trade secrets need data privacy assurances. The above highlights the need for data privacy legal frameworks in Nigeria. The periodic accusations, counter accusations, and the outright admission of the hacking of data banks of businesses/ firms[1] and state institutions[2] worldwide, including out and out international and industrial espionage, underpins the imperative for pro-privacy legal frameworks.

The foregoing begs the following questions: How safe personal data are in Nigeria? What legal frameworks are available for the protection of personal data in Nigeria? How effective are the available legal frameworks for the protection of personal data in Nigeria? Are there loopholes militating against the checking of the mischiefs these available legal frameworks for the personal data protection in Nigeria were enacted to checkmate? These questions are answered hereinafter.

* **By S.C. IFEMEJE, LLB, BL, LLM, PhD,** Professor and Dean, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, and

*** Nwafili Mark OKWUOSA, LLB, BL, LLM, PhD Candidate**, Faculty of Law, Nnamdi Azikiwe University, Awka, House of Solomon & Associates, No. 9 St. John Street, Odoakpu, P.M.B 2967, Onitsha, Anambra State.

[1]A federal grand jury indicted one Albert Gonzalez and two unnamed Russian accomplices in 2009. Gonzalez, a Cuban American, was alleged to have masterminded the international operation that stole the credit and debit cards. In March, 2010, he was dispatch to a federal prison for a 20 years stint, for his negative ingenuity. - http://www.wired.com. Last assessed on 26/7/2021.

[2]Chelsea Manning - A former U.S. Army Soldiers convicted by court - martial in July, 2013, of the Espionage Act and other offences, after disclosing to Wikileaks nearly 750,000 classified or sensitive military and diplomatic documents and imprisoned between 2010 and 2017. http://www.biography.com>people>julian assange. Last assessed on 24/7/2021.

2. Legal Framework for the Protection of Personal Data in Nigeria

There is a profundity of legal frameworks enacted to protect personal data in Nigeria, most of which insist on the globally recognized regulatory standard of fair information practice principles (fipps),[3] being the provision to visitors, of **notice, choice, access** and **security**, regarding the use of their activity data.

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

The Constitution of the Federal Republic of Nigeria 1999 (as amended) is the primary source of the right to privacy in Nigeria. Section 37 thereof provides that 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'. 'Telegraphic communications' which has since been shortened to the coinage 'Telecommunication', includes the technology by which signals, images and messages are sent over long distances by radio, telephone, television satellite, etc.[4] Clearly, internet communication is within the scope of the activities in which the privacy of the citizen is guaranteed by constitutional fiat. This constitutional foundation birthed statutory and case law supports (discussed hereinafter) for privacy rights of Nigerian residents online. The most important incidence of the constitutional root for privacy right is the fact the not even the National Assembly can successfully legislate to impede privacy right, without having such legislation easily calcified by a court's pronouncement of its inconsistency with the Constitution. It would require a constitutional amendment to tamper with such a gilt-edged (as it were) right. Constitutional amendments are not made either lightly or on the sly. Privacy right, thus, has the strongest statutory protection possible in Nigeria; hence, the other sector specific legal frameworks (discussed here after) are threading a well beaten part.

Criminal Code

Section 24, Criminal Code,[5] provides that 'A husband and wife of a Christian marriage are not criminally responsible for a conspiracy between themselves'. This is a definite statutory protection for the privacy of communication between marital partners. One cannot be successfully tried for conspiracy with a spouse; this is irrespective of the role he/she may have played in planning an offence for which the other is undergoing trial. In like manner, to preserve the right of a family or individual to their privacy and their inviolate right to be left alone, the Criminal Code Cap. 36 Laws of Anambra State, 1991, went on, at *Section 45* thereof to inure to the citizen a near absolute defence for whatever he or anyone assisting him does in defence of the privacy cum security of his dwelling house.

Torts Law

Section 176 of the Tort Law[6] provides thus: 'Publication of defamatory matter by a husband to his wife, or by a wife to her husband, or by one wife to another wife both of whom are married to the same person shall be absolutely privileged and shall not constitute publication of such material for the purposes of this part of this law (defamation)'. Yet again the privacy of people in a marriage relationship is secured and exempted from punitive reaches of the tort of defamation. Man and wife and even co-wives have their gossips over the character of a third party immune from liability.

Child's Rights Act 2003[7]

The Child's Rights Act, 2003 (hereafter referred to as the CRA, 2003) is a Child Right - specific law with unique provisions for the protection of children, including their right to privacy. A child thereunder is defined as a person under the age of 18.[8] Under it, each child's right to privacy, family life, home, correspondence, telephone discussion and telegraphic communications, subject to the supervision of the parents or guardians, is assured.[9]

National Identity Management Commission Act 2007

[3](A) Providing notice as to that individual data subject's information collected and its use or disclosure by the data custodian; (B) The choices data subjects have with regard to the collection, use and disclosure of that information; (C) The access data subjects have to that information, including to ensure its accuracy; and (D) The security of the information so collected.

[4] Oxford Advanced Learner's Dictionary, 7th Edition, p.1521.

[5] Cap. 36 Laws of Anambra State of Nigeria, 1991

[6] Cap 140 Laws of Anambra State 1991.

[7] Cap. C50, Laws of the Federation of Nigeria, 2004.

[8] Child Right Act, 2003.

[9] *Ibid.*

The National Identity Management Commission Act 2007 (herein called the NIMC Act, 2007) set up the National Identity Database[10], with the aim of identifying and building a database of registerable persons, using fingerprints with other unique biometrics, amongst other aims.[11] In order to guard against the abuse of the power to gather data under NIMC Act, 2007, its Second Schedule limited the nature of data that may be recorded and cached about a person.[12] Barring public interest considerations as in cases bordering on National Security purposes[13]; prevention and detection of crime[14]; or any other purpose,[15] as may be specified by the National Identity Management Commission (hereafter called 'the Commission'), non-disclosure of an identifiable person's data is guaranteed, except with the commission's and the data subject's consent[16] Though penalties exist to cover some offences, which penalties seem harsh,[17] the NIMC Act, 2007 yet provided hefty fines and jail term against unauthorized access of Database data.[18]

3. Nigerian Health Sector Legal Frameworks

This scholar identified two legislations in Nigeria which made ample provisions for the protection of the privacy of personal health records/ data. These legislations are discussed *anon*.

National Health Act 2014

The National Health Act 2014 (hereafter called 'the NHA, 2014') is the principal legislation in respect of the rights of patients in Nigeria, generally. On the individual's privacy of health records, the NHA, 2014, remains the most primal, and the most comprehensive statute. Under it, health institutions have a duty to record data obtained from and about the condition of each patient,[19] and data regarding to the user's status, treatment or the length of stay therein, is confidential.[20] Barring disclosure allowed in the interest of the institution's user/ patient,[21] the confidentiality grading of such data implies that it may not be disclosed, except, with either the user's written consent; a court order; with the request of a child's guardian; in the case of an incapacitated patient, on the request of a representative; or in a case where non-disclosure represents a serious threat to public health.[22] Quite unlike to what obtains in Nigerian Tertiary Hospitals,[23] access to the user's personal identifying health records is barred, even for teaching, or study purposes, without the user's consent, the concerned institution's head and the relevant health research Ethics Committee.[24, 25]

HIV and AIDS (Anti-Discrimination) Act 2014

The HIV and AIDS (Anti - Discrimination) Act 2014 (hereafter called 'the HAAD Act, 2014') was enacted to protect the privacy right, amongst other basic rights of persons living with HIV and AIDS; it boasts of a plethora of affirmative provisions in favour of the subject persons. The provisions that are relevant to the subject matter of this study are those that address the preservation of the privacy of data generated and stored on the target population. The HAAD Act, 2014, outlaws an inquiry which requires the disclosure of the HIV status of a person, as a condition to gaining access to any publicly or privately delivered service, employment and any other opportunity, privilege or right.[26] Exemptions to this non-disclosure provision exist in some cases, like marriage and cohabitation;[27] insistence on HIV testing as a condition precedent to the grant of access to public or private services or opportunities, by an employer, institution, body or person; this is, of course, subject to some exceptions.[28] In the case of bar on HIV test as a condition for employment and other privileges by both private and public institutions, there exists; subject to a case of medical testing of persons for fitness for work

[10] Section 14, National Identity Management Commission Act, 2007.
[11] Section 15 (a) - (f), National Identity Management Commission Act, 2007.
[12] Section 17 (1) [a], National Identity Management Commission Act, 2007.
[13] Section 26 (3) [a], National Identity Management Commission Act, 2007.
[14] Section 26 (3) [b], National Identity Management Commission Act, 2007.
[15] Section 26 (3) [c], National Identity Management Commission Act, 2007.
[16] Section 26 (1) [a] and (b), National Identity Management Commission Act, 2007.
[17] Section 28 (1) [b] and (c), National Identity Management Commission Act, 2007.
[18] Section 28 (1) [a], National Identity Management Commission Act, 2007.
[19] Section 25, National Health Act, 2014.
[20] Section 26 (1), National Health Act, 2014.
[21] Section 27, National Health Act, 2014.
[22] Section 26 (2) [a - e], National Health Act, 2014.
[23]Patients under admission in Teaching Hospitals and other tertiary health institutions are regularly barged in upon by their case senior doctors, with medical trainees (students and residents, alike) in tow, without any pretense at securing their consent before such visits.
[24]Section 28 (1) [b], National Health Act, 2014.
[25] Section 28 (2), National Health Act, 2014.
[26] Section 8 (1), HIV and AIDS (Anti – Discrimination) Act, 2014.
[27] Section 8 (2), HIV and AIDS (Anti – Discrimination) Act, 2014.
[28] Section 9 (1), HIV and AIDS (Anti – Discrimination) Act, 2014.

and other responsibility, a restriction.[29] Even educational institutions are barred from mandatory HIV testing as part of its routine medical test and accreditation of students.[30]The HAAD Act, 2014, precludes anonymous, unlinked surveillance or epidemiological HIV testing, executed in a manner that accords with ethical and legal principles regarding such study.[31] The test for the anonymity of lies in the answer to the question as to whether there is a reasonable possibility that one's personal identifying features could be linked to the test.[32]

4. Privacy of Personal Data in Nigerian Communication Sector

There are ample legislative efforts, particularly, in the recent time, made to address the dismal gap in the protection of the personal data of Nigeria - based communication service consumers. This scholar has identified the three statutes presently in force in this regard, and now discusses those herein, briefly.

Nigerian Communications Act, 2003

Interestingly, under the Nigerian Communications Act, 2003, (hereafter called 'the NCC Act'), the functions of the Nigerian Communications Commission (hereafter called 'the Commission') include, 'the protection and promotion of the interest of consumers against unfair Practices….'[33] The Minister in charge of Communication, has his functions described to include the formulation of policies;[34] these are wide powers to regulate this sector, if put to good use. The Commission enjoys sufficient powers to gather and cache data; and wide powers to compel 'a person subject to the Act' to furnish it with any data that it may request, however, it failed to define 'a person subject to the Act.'[35] Unfortunately, the word 'person' was widely and inclusively defined thereunder to include 'corporate bodies and partnerships.'[36] There is a lot that the Commission could do for the protection of data privacy with such persons, against all manner of entities - natural and artificial. Indeed, the Commission is required to keep registers with absolute discretion to release the content thereof to the members of the public, at a cost.[37]

Consumer Code of Practice Regulations, 2007

The Consumer Code of Practice Regulations, 2007 (hereafter called 'the CCPR, 2007') places a restraining hand on the Telecommunication firm/ licensee on the data it could collect and cache on a consumer, which data should be reasonably necessary and required for its business purposes by providing certain fair information practice guidelines.[38,] The CCPR, 2007, surely made a quantum leap, given where we are coming from. Though, there is need for consumer vigilance so that the necessary update of the Code would be regularly carried out to keep pace with the fast - paced information technology arena, as well as, with the nuances of the ever profit conscious telecommunication operators. Unsolicited messages from online based firms, driven by unbridled pursuit for competitive edge via telemarketing, is another notorious way of violating subscribers' data privacy right.[39] Happily, Nigerians are gradually rising to the occasion of this mischief. In *Godfrey Nya Eneye v. MTN Nigeria Communication Ltd,*[40] the plaintiff, a legal practitioner, having had enough of unsolicited messages from commercial interests, sued the defendant - telecommunication company, claiming a breach of his right to privacy under the 1999 Constitution, [41] on account of the unauthorized disclosure of his personal telephone number to the unknown third party firms. On 2/11/2016, with the Hon. Justice Jude Okeke (recently deceased) then of the Federal Capital Territory High Court, Abuja, presiding, the court found in favour of the plaintiff, awarding damages to the tune of N5, 000, 000. 00, against the defendant - Telecommunication Company In another matter with facts similar to those of the *Eneye case*, another subscriber- Ezugwu Emmanuel Anene, sued Airtel Nigeria Ltd. to which services it subscribed, for the unauthorized disclosure of his private phone numbers to third parties, who bombarded him with calls and solicitous messages to his immense discomfiture.[42] Again, the court found that the defendant's conduct breached the constitutionally assured right of the plaintiff to privacy, and restrained the defendant from such further breaches, along with a N5, 000, 000. 00 damages. The

[29] Section 9 (5), HIV and AIDS (Anti – Discrimination) Act, 2014.
[30] Section 9 (2), HIV and AIDS (Anti – Discrimination) Act, 2014.
[31] Section 12 (1), HIV and AIDS (Anti – Discrimination) Act, 2014.
[32] Section 12 (2), HIV and AIDS (Anti – Discrimination) Act, 2014.
[33] Section 4 (b) of the Nigerian Communications Act, 2003.
[34] Section 24 of the Nigerian Communications Act, 2003.
[35] Sections 64 - 67, of the Nigerian Communications Act, 2003.
[36] Sections 157, of the Nigerian Communications Act, 2003.
[37] Sections 68 and 69, of the Nigeria Communications Act, 2003.
[38] Code 35 (1& 2) Consumer Code of Practice Regulations, 2007.
[39]Chukkol, O.G, Rights of Consumers/ Subscribers of Telecommunications Services in Nigeria (Webinar Presentation Faculty of Law, Ahmadu Bello University, Zaria, 23rd March, 2020), P. 10.
[40] (Unreported), Suit No. FCT/ HC/ CV/ 545/ 2015 -
[41] Section 37. Chukkol, O.G, Rights of Consumers/ Subscribers of Telecommunications Services in Nigeria (Faculty of Law Webinar, Ahmadu Bello University, Zaria, 23rd March, 2020), P. 10.
[42] Ezugwu Emmanuel Anene v. Airtel Nigeria Ltd. (2018) LPELR - 44447 (CA).

defendant unsuccessfully appealed the trial court's judgment, but further appealed to the Supreme Court, which judgment is still eagerly awaited, as it would, no doubt grow the law. It has been opined that a data controller could protect itself from liability for disclosure, if it secures the data subject's consent at the point of the initial processing of such data and contract; provided that the purposes are stated at the time of the data collection.[43] So long as such practice leaves the subject an option to grant or withhold such a permit, we find it good enough.

Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations, 2011

One of the two expressed objectives of the Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 (hereafter called 'the RTSR, 2011'), is the 'establishment, control, administration and management of the Central Database.'[44] The RTSR, 2011, defines the 'Central Database' as 'a database of all registered subscribers' information.'[45] Generally, access to subscribers' data is restricted, subject to the right of access thereto by security agencies, in their line of duty. Access is made subject to the submission of a written request to the Nigerian Communications Commission, by an officer of the Security agency concerned, not be below the rank of Assistant Commissioner of Police/ its equivalent in the other security agencies.[46] Even at that, a release that may infringe on the Constitution, an Act of the National Assembly; or one threaten national security,[47] is not permitted. In line with the global fair data control practices, and the constitutional guarantee of the right to privacy, [48] the RTSR, 2011, provides for the traditional safeguards and confidentiality in the control of subscribers' personal data held in the Central Database.[49,50,51,52, 53,54 and 55]

5. Evidence Act 2011 (As Amended) [56]

The Evidence Act 2011, subject only to a few reasonable exceptions, protects the privacy of communication between husband and wife/ wives during marriage.[57] It also protects against compellability to reveal in a court trial situation, information accessed under circumstances covered by professional privilege, i.e.: Attorney - client relationship.[58] Legal practitioners under the Evidence Act, subject only to reasonable exceptions, are thus immune from compulsion to disclose information brought to their knowledge in the course of their professional interactions with their clients. Indeed, it amounts to professional malpractice for the legal practitioner to reveal such privileged information.[59] Likewise, albeit no similar protection exists under the Evidence Act, in respect of a medical doctor/ patient communication, it is a violation of the rules of professional conduct for a medical doctor to divulge sensitive information about patients, such as relates to 'criminal abortion, venereal disease, attempted suicide, concealed birth and drug dependence.' [60] Even upon a judge's order, the medical doctor, under the medical rules of professional conduct, is only allowed to obey such order 'strictly under protest.'[61] The Freedom of Information Act (as shall be seen below) has remedied this mischief of lack of statutory force behind this health workers' privilege. Even the men of the cloth/ priests, though not protected under the Evidence Act, either, are equally bound by strict ethical codes regarding information that may come to their knowledge in the course of their pastoral office.

6. Freedom of Information Act, 2011

Even the Freedom of Information Act, 2011 (hereafter called the 'FOIA, 2011'), which main aim is to grant the public access to data in the custody of public bodies/ institutions, commendably made exemptions in respect of data that borders on or that may entail the exposure of personal data. The FOIA, 2011 provides against the

[43]Nwankwo, Iheanyi, *Nigeria's Data Privacy First Responders* (Consumer Protection, Data Protection, ICT Law, Uncategorized, April 4, 2018), p. 7
[44] Regulation 2 (b), Registration of Telephone Subscribers' Regulation, 2011.
[45] Regulation 4 (a), Registration of Telephone Subscribers' Regulation, 2011.
[46] Regulation 8 (1) and (2), Registration of Telephone Subscribers' Regulation, 2011.
[47] Regulation 10 (2), Registration of Telephone Subscribers' Regulation, 2011.
[48] Section 37, Constitution of the Federal Republic of Nigeria, 1999 (as amended).
[49] Regulation 9 (1), Registration of Telephone Subscribers' Regulation, 2011.
[50] ·Regulation 9 (2), Registration of Telephone Subscribers' Regulation, 2011.
[51] Regulation 9 (3), Registration of Telephone Subscribers' Regulation, 2011.
[52] Regulation 9 (4), Registration of Telephone Subscribers' Regulation, 2011.
[53] Regulation 9 (6), Registration of Telephone Subscribers' Regulation, 2011.
[54] Regulation 10 (3), Registration of Telephone Subscribers' Regulation, 2011.
[55] Regulation 10 (4), Registration of Telephone Subscribers' Regulation, 2011
[56] Cap HB. 214, Laws of the Federation, 2004.
[57] Section 187 (1), Evidence Act, 2011 (as amended).
[58] Section 192 (1), Evidence Act, 2011 (as amended).
[59] Rule 19, Rules of Professional Conduct, Legal Practitioners' Act, 2007.
[60] Nigeria Medical Association Guideline Part D, Section 44.
[61] *Ibid.*

disclosure (by public institutions) of information which contains personal data, except in the event that the data subject consents, or the information, albeit entails the disclosure of personal data, is already in the public domain.[62] Under the FOIA, 2011, communication between a patient and health workers remains privileged, thus health institutions are empowered to deny/ ignore any request for such data.[63] The FOIA, 2011, generally exempts the disclosure of information from its operation, disclosure of which would constitute an unwarranted invasion of personal privacy.

7. Federal Competition and Consumer Protection Act 2019

Quite recently, the Federal Competition and Consumer Protection Act, 2019 (hereafter called the 'FCCPA, 2019'), was commendably introduced, providing protection for trade secrets that are wont to be exposed in the course of the investigation of a complaint of the piracy of one's trade secret by another - industrial espionage, amongst other objectives. The FCCPA, 2019, birthed the Federal Competition and Consumer Commission, vesting it with powers to receive and investigate complaints from co - competitors and consumers alike. In doing so, the FCCPA, 2019, is bound to ensure the protection of business secrets of all parties involved in the investigations it may conduct, and to do so through all phases of the inquiry/ investigation.[64]

8. Privacy of Personal Data in the Nigerian Financial Sector

A few financial sector instruments have been introduced either by the Central Bank of Nigeria as delegated legislations, or enacted by the National Assembly, with the intent of further regulating the financial sector, as it concerns the control of the personal data of consumers of the products in that sector. We shall now consider two of such instruments relevant here at.

Credit Reporting Act 2017

The Credit Reporting Act, 2017 (CRA, 2017) was enacted on the 30th day of May, 2017, primarily to enhance access to credit information and improve risk management in credit transactions. This, understandably, entails the processing, the caching and the sharing of the personal data of bank debtors, as a means of ascertaining high risk borrowing prospects. Wherever personal data is processed the next challenge is usually how to manage such data in order to obviate or control the possibility of misuse of such personal data. To this end, the CRA, 2017, in tandem with the best global standards, provided for the fair information practice principles (fipps), including mechanisms for seeking redress by an aggrieved data subject.[65] The personal data of credit bureau creditor subjects are assured of a level of protection that was not possible in Nigeria before the enactment of the CRA, 2017, should the provisions thereof be enforced to the letter.

Consumer Protection Regulations 2019

The Central Bank of Nigeria, on the 7th day of November, 2016, introduced the Consumer Protection Framework, with the expressed object of enhancing consumer confidence in the financial services industry and promoting financial stability, growth and innovation. Then, in keeping with the objects of the said Consumer Protection Framework (hereafter called 'the CPF'), the Central Bank of Nigeria (hereafter called 'the CBN'), on the 20th day of December, 2019, pursuant to her supervisory powers under the Central Bank Act, 2007,[66] and the Bank and other Financial Institutions Act, 1991 (BOFIA, 1991) [67] introduced the Consumer Protection Regulations, 2019 (hereafter called the 'CPR, 2019'). The CPR, 2019, was introduced to, amongst others; ensure the fair treatment of consumers. Some of the provisions thereof address the need for the confidentiality of the data supplied by and processed from consumer data subjects; those are our interest in this research. The CPR, 2019, made provisions for the privacy and protection of the personal data of the consumers of financial services in Nigeria.[68] I adjudge these provisions as detailed, adequate and standard in compliance with global fair information practice principles (fipps).[69] The provisions made the standard provisions for the confidentiality of data; the written consent of the data subject before processing his personal data; transfer of data to third parties subject to data subject's consent, except in cases of overriding legal obligations; notice to data subject in the event of authorized transfer to a third party; review of data application to ensure compliance with the purposes of initial consent; and maintenance of accuracy and right to correct and update data.

[62] Section 14, Freedom of Information Act.
[63] Section 16 (B), Freedom of Information Act.
[64] Section 34 (6), Federal Competition and Consumer Protection Act, 2019.
[65] Setions 6 (a) - (g), 12 and 13, Credit Reporting Act, 2017.
[66] Section 54, Central Bank of Nigeria (Establishment) Act, 2007.
[67] Sections 61, Banks and other Financial Institutions Act, 1991, Cap. B3, Laws of the Federation, 2004.
[68] Section 5.4, Consumer Protection Regulations, 2019.
[69] See Page 14, *ante*.

9. Nigeria Data Nigeria Data Protection Regulation 2019

The Nigerian main data privacy protection instrument, outside the Constitution, is the recent Nigeria Data Nigeria Data Protection Regulation, 2019 (NDPR, 2019). This recent regulation is a subsidiary legislation made by the National Information Technology Development Agency (NITDA), which was itself created under the National Information Technology Development Agency Act (NITDA Act). The Nigeria Data Protection Regulation Implementation Framework, not unlike most of our laws, is an adaptation of a law enacted elsewhere; this time around, the European Union – the General Data Protection Regulation (GDPR). The NDPR, unlike the prior personal data regulatory instrument, which are essentially sector-specific, is a fairly comprehensive and reasonably generalized personal data protection, control and regulation instrument. It is the most personal data specific legal instrument in Nigeria. Amongst the laudable objectives of the NDPR, 2019, is the safeguarding of the rights of natural persons to data privacy; [70] and the prevention of the manipulation of personal data.[71] 'Personal Data Breach' was defined by the regulation in a manner that placed a strict liability for any such breach on the data custodian; [72] the data custodian is liable, even for an 'accidental' destruction or loss of data. Processed data must not be stored for an unreasonably long period. All of the foregoing, notwithstanding, whoever processes such personal data under legitimate situations, yet bears the duty to secure such data against 'all foreseeable hazards and breaches such as theft, cyber-attack, viral attack, dissemination, manipulation of any kind, damage by rain, fire or exposure to other natural elements.' [73] To this end, the data controller is expressly tasked by the NDPR, 2019, to develop security measures for the protection of personal data in his custody from those threats, by setting up firewalls, encryption technologies, and continuous data security capacity building, amongst others.[74] There is an express obligation of a duty of care [75] and accountability [76] on every custodian, for the benefit of the data subject. There is a clause for, notwithstanding other provisions of the NDPR, 2019, the mandatory and conspicuous display of privacy policy, and in a manner that the data subject could understand, due regard being had to the class/ level of the target data subjects. Privacy policies are notoriously tiny in font, labourious, and complicated in presentation. Their standard presentation seems to have been designed to discourage from reading them users. It has been suggested that the time site visitors use to read them be economically assessed and paid for.[77]

In the bid to continually advance privacy rights of personal data subjects, the NDPR, 2019, expressly provided that privacy rights of a data subject shall be interpreted to advance (not to restrict) the safeguards available to a data subject under any instrument made in furtherance of the fundamental right to privacy under the Nigerian Constitution and other Nigerian laws.[78]Commendably, and in a positive shift from the usual Nigerian legislative laxity in tackling foreign interests, the NDPR, 2019, adopted a principle of adequacy of reciprocal data with the Nigeria Data Nigeria Data Privacy Regulations, in matters of transfer to a foreign country. Such conditions that qualify as adequate regulations in the foreign country under the circumstance include: the presence of structures that ensure adequate protection for personal data privacy; a legal system that respects the rule of law, fundamental rights, etc.; regulated third party country transfer; the presence of independent supervisory authorities and assistance to subjects in seeking redress; and the evaluation of international obligations of the foreign country. The data subject enjoys, of course, the right of unrestricted access and portability/ transfer of any personal data processed by a data controller, to any other controller, agency, foreign nation, etc., without restrictions or hindrance by the data controller who processed it. The only limit to this right is where the personal data in question was processed in pursuance of a task carried out in public interest, or in the exercise of official authority vested in the controller.[79] Under Chapter Three of the NDPR, 2019, provisions, which this scholar deem adequate for the time being, were made stipulating mechanisms (practical steps) for the implementation of the rights, duties and obligations thereunder.[80,] However, as salutary as the NDPR, 2019 may be in its reasonable timeliness and content, it is not without its pitfalls. A bit of confusion was introduced in the very first chapter thereof: While amongst the objectives of the regulation was 'to ensure that Nigerian

[70] Regulation 1.0 (a), Nigeria Data Nigeria Data Protection Regulation, 2019.
[71]Secion 1.0 (b), Nigeria Data Nigeria Data Protection Regulation, 2019.
[72] Section 1.3 (s), Nigeria Data Nigeria Data Protection Regulation, 2019.
[73] Section 2.1 [1] (a), (b), (c) and (d), Nigeria Data Nigeria Data Protection Regulation, 2019.
[74] Section 2.6, Nigeria Data Nigeria Data Protection Regulation, 2019.
[75] Section 2.1 [2], Nigeria Data Nigeria Data Protection Regulation, 2019.
[76] Section 2.1 [3], Nigeria Data Nigeria Data Protection Regulation, 2019.
[77] McDonald, A.M and Cranor, L.F, The Cost of Reading Privacy Policies. (A Journal of Law and Policy for the Information Society, 2008 Privacy Year in Review Issue) P. 2.
[78] Section 2.5, (a) - (i) Nigeria Data Nigeria Data Protection Regulation, 2019.
[79] Section 2.13.14, Nigeria Data Nigeria Data Protection Regulation, 2019.
[80] Section 2.13.15, Nigeria Data Nigeria Data Protection Regulation, 2019.

businesses remain competitive in international trade…,' [81] the description of the scope of the regulation limited its application to natural persons only.[82] Trade secrets, just like personal privacy, are no longer adequately protected in this age of the internet, given the reach and extra- territoriality of the latter; hence, the need to have the extra covering extended to businesses and organisations, too.

Another curious twist in the couching of the scope of the NDPR, 2019, is that its effect is limited to 'natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent'.[83] Impliedly, foreigners who wish to engage Nigeria and Nigerian businesses from their bases outside Nigeria would be risking the unbridled breaches of their data privacy, without any recourse to the Nigerian courts for protection. That is hardly a prime example of how to attain the 'global best practices'[84] advertised as one of the objectives of the NDPR, 2019. The focus has always been on breaches of data privacy by public bodies, while such breaches by private entities have continued to fly under the radar; remaining beyond the reach of data protection legislations and institutions. [85]

10. Conclusion and Recommendations

The extant legal frameworks for the protection data privacy rights in Nigeria are fairly sufficient for their purposes. With vigilance, any informed consumer of health, telecommunications or financial services in Nigeria has a guarantee of the confidentiality of his personal data, and, in the event of a breach, a means of accessing redress. Data privacy protection laws are public sector-centred, thus leaving private firms, most of which handle substantial quantum of private data out of reach. The NDPR, 2019 did not fulfill its objective international competitiveness of Nigerian businesses by limiting its application to natural persons, the achievement of the stated aim might remain unattainable, because of the exclusion of the data of corporate bodies from protection. The effect of the NDPR, 2019, is limited to 'natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent'. Foreigners, who engage or may wish to engage Nigerians or Nigerian firms in business relations from their bases outside Nigeria, are exposed to boundless and irredeemable breaches of their data privacy, without remedy from Nigerian courts. The present state of affairs, which requires that the customer of a financial institution could to have done more to protect his personal data from being delivered to a third party in a manner that breaches his data privacy right, does not seem fair in a backward society like ours. It is recommended that the NDPR, 2019 be reviewed to protect the confidential data of businesses, too. Trade secrets are also under grave threat of undue exposure in this internet age. Another aspect that the suggested amendment of the NDPR, 2019, needs to cover, in order to boost foreign investments into the Nigerian economy and achieve the 'global best practices', is the lack of protection for foreigners engaging Nigerian businesses and businessmen. The *C.P.P.A, 2015* should be amended to ensure that the Cybercrime Advisory Council (hereafter called 'the council') is comprised of experts in the relevant field of internet and related fields, as against the present provision[86] , which is open-ended.[87] The *C.P.P.A, 2015* – designated period of 2 years' [88] data traffic and subscriber data retention period of all traffic data, should be amended to 5 years, at least, given the long delays in court trials in Nigeria, which is way above two years, even in courts of summary jurisdiction. Contrary to the *status quo*,[89] it is recommended that legislative changes be made in order to place, on financial institutions, the burden of justifying third party rendering of a client's data. The National Judicial Council, which supervises judges and oversees their on-the-job training, should liaise with relevant government agencies to ensure the regular training and upgrade of the judges' knowledge and understanding of the unique, the dynamic and advancing frontiers of the internet and its regulatory framework. The right of access to the *internet*, and the right to free expression on the internet, should undergo amendments to upgrade them, alongside the right of reasonable expectation of privacy of personal data on the internet, among other ancillary rights, to basic constitutional rights. Laws should be enacted to compel cyber-based entrepreneurs desirous of doing business with Nigerians and Nigeria-based firms to present a summarized, informative and generally, user friendly versions of the mandatory privacy policies.

[81] Section 3.3.1 (a), (b), (c) and (d), Nigeria Data Nigeria Data Protection Regulation, 2019.
[82] Section 1.0 (d), Nigeria Data Nigeria Data Protection Regulation, 2019.
[83] Section 1.2 (a), (b), (c), Nigeria Data Nigeria Data Protection Regulation, 2019.
[84] Section 1.2 (b), Nigeria Data Nigeria Data Protection Regulation, 2019.
[85] Bygrave, Lee .A, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties (*International Journal of Law and Information Technology*, 1998, Vol. 6), pp. 247 – 284.
[86] *First Schedule, Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.*
[87] *Section 42 (2), Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.*
[88] *Section 38 (1) and (2), Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.*
[89] *Section 19 (3), Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.*