(2022) 29 JUUM 3 - 16
https://doi.org./10.17576/juum-2022-30-01

Data Privacy Rights and Bankers' Business Interests in Nigeria: Reflections on Opportunities, Challenges and Legal Reforms

Abdulkadir Bolaji Abdulkadir
Abdulfatai Oladapo Sambo

ABSTRACT

Data (Personal Information), the oil of the digital age, has taken the centre stage due to increasing use of technology in almost all human endeavours. This is not unconnected to the large scale unlawful usage of people's data by cyber criminals. This is particularly the situation in banking sector. Yet, Nigeria seems to be lagging behind in its efforts to protect this right through effective legislative framework to protect individual information from unlawful and unauthorised possession or use. Nonetheless, efforts are on top gear at the global level to stem this ugly tide. Therefore, this paper seeks to investigate the Data Protection challenges in the Nigerian banking sector with critical analysis of the current legal framework for the protection of personal information in the Nigerian banking sector. Using doctrinal methods where primary and secondary sources of legal materials were subjected to content analysis, the study found that legal architecture on data protection in Nigeria is weak and ineffective in stemming the tide of the challenges posed by data challenges. It was also concluded that effective legal framework on data protection is necessary for the enjoyment of the opportunities of this digital age. The study thus recommended that there should be effective data protection legislation in Nigeria particularly in the banking sector that would protect data privacy as well as the legitimate business interests of bankers.

Keywords: Data privacy; bankers; rights; privacy; protection

INTRODUCTION

In this digital era, data has been referred to "as the oil of the digital era."[1] It is the cornerstone of the information economy.[2] It does not go beyond a mere business handling tool. It appears even more valuable than physical assets. This is especially the situation in financial and banking sectors where acquiring personal data as well as the adoption of information technology (IT) have both transformed the banking sector together with the associated operational risk management.[3] Every second, millions of individual data is collected, processed, stored and accessed by players in private as well as public sector. This has brought the importance of protecting personal data and information to the forefront in any privacy rights discourse. Bearing the above in mind, there has been national, regional and global efforts to protect data. For instance, the right to private life is a Fundamental Human Right guaranteed by the Constitution of Nigeria in section 37 and other international instruments.[4] Also, there are currently 17 African States[5] with comprehensive personal data privacy legislation.[6] In addition, the African Union (AU), adopted the AU Convention on Cyber security and Data privacy in June 2014 but not yet in force. At the moment, Nigeria intends to enact legislations relating to personal data privacy. With the improved involvement of technology in the global banking industry, the need for a justly balanced law in order to protect customer's information has gained momentous attention.[7] Moreover, the General Data Protection Regulation (GDPR), with its coming into effect in May 2018, much concentration has been on various sectors that will be affected by the new regulations especially the financial sector. Many European nations have amended their data privacy laws to meet the new standards created by the regulations. With over 74 million active bank accounts in Nigeria,[8] the banking sector has become a very important sector in the Nigerian economy. While discussions on protection of customer's data especially in the financial sector have been on for a number of decades, a lot of attention was drawn to it when the Central Bank of Nigeria (CBN) made a circular which mandates all bank customers to have a Bank Verification Number (BVN) in 2014.[9] It is against this background that this study assesses the present framework for the protection of the right to data privacy and how best to protect, promote and enforce this right. Therefore, this paper is divided into five parts including the introduction. The

second part discusses the nature of data protection and its associated issues in banking sector. The third part examines the challenges associated with data protection in Nigerian banking sector. The fourth part examines the legal framework on data protection in the Nigeria's banking sector. The last part concludes the paper and suggests the needed legal reforms.

WHAT IS DATA PROTECTION?

Writers usually concur to the term "data protection" in Europe – the terminology that is generally used in this study. In other jurisdictions away from Europe, "data privacy", "privacy" or "information privacy" seems to be the preferred terminology.[10] Notwithstanding these terminological differences, this study focuses on regulation of data concerning identification of, persons (i.e., personal data) in order to protect the privacy and other individual's related interests. In this regard, European Data Protection Supervisor noted that:

> "Data protection is about protecting any information relating to an identified or identifiable natural (living) person, including names, dates of birth, photographs, video footage, email addresses and telephone numbers. Other information such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered personal data."

Data protection laws essentially afford individuals the right to personal data protection. The term "data protection" is coined from a German word "*Datenschuz*." It serves a wider range of interests beyond mere privacy protection.[11] Accordingly, De Hert and Gutwirth, noted that data protection, though difficult to summarise in a few words, can be said to be "a catch-all term for a series of ideas regarding the processing of personal data."[12] In the words of Akinsuyi, "Data protection involves the implementation of administrative, technical or physical measures to guard against unauthorised access to such data."[13] Whether it is data privacy or data protection, what is important is the law need to regulate the use of 'personal data' by several establishments in order to protect individual rights by protecting the use of data from abused by various organisations.

THE PRIVACY VERSUS DATA PROTECTION DEBATE

There is a thin line of distinction between the right to protection of personal data and the right to privacy. In other words, privacy and data protection are two controversial concepts in privacy discourse. This is the reason why it is lightly assumed that the two ideas represent two sides of the Atlantic. As earlier pointed out, the usages depend on jurisdictions. In the USA, for instance, the use of privacy is common. In Europe, data protection is of common usage.[14]Some authors argue that the terms can be used interchangeably as it is synonymous while some differ. Cuijpers also questions the difference between data protection and privacy.[15]De Hert and Schreuders opine that the two concepts are not identical although they share certain characteristics and vision.[16] They are thus described as un-identical 'twins'. They further submit that data protection may not necessarily raise privacy issues though deep seated in privacy protection. At least, 160 countries provide for right to privacy in their constitutions. Nonetheless, the understanding of the term privacy varies significantly from one country to another. The distinction is usually based on culture, historical background, and philosophical differences. This account for different methods and approaches in the protection of data in many countries. In many legal traditions, privacy includes the inviolability of homes, correspondences, and family life. In fact, the 28 member states of the European Union (EU) recognised data protection as a fundamental right guaranteed in the 2001 EU Charter[17]

DATA PRIVACY PROBLEM IN THE NIGERIAN BANKING SECTOR.

Undoubtedly, one sector where huge volume of data is gathered in Nigeria is the banking sector. The financial activities and personal information of customers are usually collected and stored. It is even more common in the present regime of electronic banking. This has been an inevitable banking practice in recent times. The nature of required information includes full name, account number and passwords, residential address, BVN, passport number and so on. This information is sensitive and requires serious protection. Otherwise, it could be stolen by thieves, bandits, kidnappers, terrorists, fraudsters and other forms of criminals. Nigeria faced over 4,000 cyber-attacks with 70 per cent success rate and loss of about $500 million in recent years mainly via cross-channel fraud, data theft, email spoofing, phishing, shoulder surfing and underground websites.[18] There is therefore a compelling need for banks to enhance data protection due to huge sabotage in security network and the risks associated with identity theft

and fraud. The fraudsters target the banks more than any organisation.

In order to protect bank customers' rights particularly in matters relating to electronic banking, the Central Bank of Nigeria (CBN)[19] in August 2003 issued its Guidelines which seek to address "(i)information and communications technology standards on security and privacy; (ii)monetary policy; and (iii) legal guidelines on banking regulations and consumer rights protection; and regulatory and supervisory issues." Besides, there is the CBN Guidelines for Card Issuance and Usage 2014 which places heavy burden on banks to secure cards issued to its customers. The guideline provides that: "'The security of the payment card shall be the responsibility of the issuer and the losses incurred on account of breach of security or failure of the security mechanism shall be borne by the issuer, except [where] the issuer establishes [responsibility for the] security breach on the part of the card holder."[20] It further states that "Issuers should ensure that the process of card issuance is completely separated from the process of PIN issuance, and done in accordance with best practices thus minimizing the risk of compromise."[21] Some of the main issues in the Nigerian Banking sectors are considered below:

KNOW YOUR CUSTOMER (KYC) POLICY

KYC policy is a policy in the Nigerian banking sector that is aimed at knowing customers. In January 18, 2013, the CBN directed banks, through a circular, to introduce a "three-tiered KYC requirements."[22]Prior to this circular, recognition is given to access to simple banking facilities as well as other financial services that are necessary in realizing the financial inclusion policy of the CBN. With the three-tiered KYC policy, the banks implement flexible account opening requirements systems particularly for low-value and medium-value account holders though subject to caps and transaction limits. This would ensure that persons disadvantaged as a result of finance and social status are not prevented from opening accounts or getting other financial services for lack of suitable means identification. The personal data of the customers are updated through the KYC policy. This policy however raises serious concern on data protection as the data can be used for ulterior motives or even sold to retailers or direct marketers who may use it for advert placement. Banks may also use it for marketing, unsolicited, of its products to customers.

THE BANK VERIFICATION NUMBER (BVN) SCHEME

In furtherance of KYC policy, the CBN, in 2014, mandated all bank customers to register for a BVN. The scheme, as at May 2018, registered about 34million Nigerians to the scheme. Bank customers were made to fill intricate forms which required much personal information of customers including but not limited to photographs and biometric data. Despite the outcry against the scheme against the backdrop of inadequate data privacy protection framework in the country, the scheme continued.[23]The Paradigm Initiative in fact demanded for detailed data privacy laws before people can be asked to register for BVN.[24] The letter sent to CBN reads in part: "The Bank Verification Number (BVN) upon perusal seeks to expose confidential information of private citizens and is also riddled with severe implications since there are no legal frameworks in place to safeguard the data collection exercise." Many concerns raised also include "Who do we hold accountable when there's a breach? How secure is our data? What kind of system is protecting the data from illegal access? What constitutes illegal access to this data? Why can't there be information sharing across the several agencies? Who is the CBN accountable to, when it comes to the BVN?"

ELECTRONIC BANKING (E-BANKING)

E-banking may be described as a means whereby electronic devices and automated processes are used in banking transactions. These processes and devices include telephones, personal computers, internet fax machines, and card payments. Banks use electronic banking transactions for activities such as information dissemination, account balance check-up, funds transfer and so on.[25]Banks were hitherto paper based prior to these modern transaction systems. It was purely bank notes, payment orders, and the use of cheque books. The transformation of the payment system practically started in 1996 with CBN's approval of a closed system of electronic purse to banks. The banks, particularly Diamond Bank, then introduced 'paycard' in February 1997. In 2003, the CBN, in partnership with the Bankers Committee, approved for banks telephone banking, international money transfer products and online

banking via the internet on a limited scale. Currently, almost all banks have put in place electronic funds transfers (EFT), internet banking, mobile banking debit and credit cards, and the use of Automated Teller Machines (ATM) is all over the country.

The Nigerian E-banking system has developed more with the putting in place of the Payments System Vision 2020, launched in 2007. The purpose was to promote a broader range of electronic payment systems such as PoS terminals, which was facilitated by many service providers. This has also created a lot of direct and indirect jobs to the Nigeria youths who engage in PoS business. This has thus made E-banking an essential part of modern-day banking services. Globally, banking industry is mainly technologically or electronically driven. This has greatly assisted in delivering quality services to customers. Dawson[26]noted speed operation, improved product quality, time management, better communication, and competitive advantage as important components of modern-day e-banking. In the view of Olusegun, Ishola and Hammed,[27]"the transformation from the traditional banking to E-banking has been a 'leap' change, there is however a high level of job insecurity among employees in the modern-day banking industry." This implies that emphasis is currently being laid by banks on technological innovations in order to improve service delivery and customer satisfaction. Undoubtedly, those with the required technological skills are being employed thereby decreasing the level of unemployment in the country.[28]Nonetheless, and in line with the aphorism that every good thing comes with its own side effects or negatives, customers have expressed serious worries over continuous frauds that are happening in the banking industry. Financial transactions have largely become insecure series of bank fraud as a result of many internet fraudsters (Yahoo.boys) hacking into the website of the banks.

LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA IN THE NIGERIAN BANKING SECTOR

It must be said from the on-set that Nigeria does not have a comprehensive piece of legislation which provides broad data protection principles covering all sectors involved in personal data processing. Despite this, Section 37 of the Constitution of the Federal Republic of Nigeria (CFRN) 1999 provides for citizens' right to private and family life: "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected". This is the background for the protection and safeguard of citizens' privacy. Nevertheless, the Constitution does not specifically explain the scope of the term 'privacy."[29] However, some legislation has connection with data protection in Nigeria. They include: The Credit Reporting Act 2017 which provides for protection of data received by financial institutions from borrowers through credit bureau. Another one is the Cybercrimes Act 2015.Its purpose is to protect critical national infrastructure, to regulate the use of internet and computer-based information, and to prevent crime connected thereto. There is also the NITDA Guidelines for Nigerian Content Development in Information and Communications Technology (the NITDA Guidelines) 2013, the NITDA Guidelines for Data Protection 2019, CBN Guidelines for Card Issuance and Usage 2014, NITDA National Information Systems and Network Security Standards and Guidelines 2013 etc. Some Bills are nevertheless pending before the National Assembly. They include the Data Protection Bill[30] and the Personal Data and Information Protection Bill. [31] In this segment, the focus of the study's discussion will be to examine the legislations and guidelines on the financial sector and investigate the extent to which these frameworks protect data privacy in the Nigerian banking sector.

CONSTITUTIONAL PROTECTION OF DATA PRIVACY IN NIGERIA

The right to privacy is enshrined in Section 37 of the Constitution. The section provides that "*The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.*" This section appears to be rather brief with subsections or proviso to explain the scope of the fundamental human right unlike its other counterparts. There is however no specific provision for protection of personal data and information in the constitution. As earlier argued, the right to protection of personal data is very closely linked to, but different from the right to privacy. Thus, while there is no specific constitutional provision which guarantees the right to data privacy, it can be said that section 37 of the Constitution could be interpreted to also apply to personal data protection. This is because the constitution's express reference to citizens' "correspondence, telephone conversations and telegraphic communications" shows an intention by

the Constitution to protect information privacy. The greatest limitation of section 37 in protecting both privacy and data protection is that it applies only to citizens of Nigeria, thus it is arguably discriminatory.

CREDIT REPORTING ACT OF 2017

On May 30, 2017, the Credit Reporting Act ('the Act') was enacted. The aim of the Act is to promote access to credit information and enhance the principle of risk management in credit transactions.[32]In furtherance of these objectives, the Act makes provision for regulation and licensing of Credit Bureau. It also provides for the processes that would make the stake holders create, maintain and share credit information amongst themselves.[33] The Act assures Data Subjects of their rights to confidentiality, privacy, and protection of their Credit Information[34.] Further, the Act prohibits the Credit Bureau from divulging information which relate to data subjects to Credit Information without the written consent of a Data Subject in a way that is satisfactory to the Credit Bureau[35]; or "who have entered into a Data Exchange Agreement with the Credit Bureau, and where the disclosure is for a permissible purpose, of a Data Exchange Agreement with it".[36]Nonetheless, what amounts to the term "satisfactory form of consent" is not clear. Happily, the Act defines consent "as an authorization by the Data Subject, or his/her legal representative or authorized agent indicating his/her approval to inquire about his/her data from the Credit Bureau."[37] The Act imposes on Credit Bureau an obligation to create and maintain a database of credit-related information, receive and compile credit related information from Credit Information Providers (CIPs), Credit information Users (CIUs) and such other persons as the CBN may prescribe[38], regularly update their database concerning the nature of information kept whenever the information is provided by a Credit Information Provider.[39] Credit Bureau operators are required to implement strict quality control measures in order to promote the quality of information supplied as well as the continuity of their services. Similarly, a Credit Bureau, in performing its functions, especially when dealing with credit related information, must ensure the security and confidentiality of its data[40]. Nevertheless, the Act has not placed duty on a Credit Bureau to verify the accurateness of the received credit information except such information appears to be manifestly inaccurate, incomplete or misleading.[41]Information such as political affiliation, race, ethnicity, colour, religion must not be included either in credit report or data format.[42]The Act provides that a Credit Information User may seek Credit Information for permissible Purpose including carrying out Know Your Customer checks on any person for any permissible purpose or as may be required by law[43.] The KYC Scheme is one of the schemes engaged by Nigerian banks to obtain information about their customer in order to tailor banking services.

THE CYBERCRIMES ACT 2015

The Cyber Crimes Act ("the Act") is not a data protection instrument in the real sense. The Act provides for an effective, unified and inclusive legal, regulatory and institutional framework which seeks to prohibit, detect, prevent, prosecute and punish cybercrimes in Nigeria. The primary purpose of the Act is to "promote cyber security and protection of computer systems and networks, electronic communications, data and computer programs intellectual property and privacy rights."[44] Section 38 of the act provides that:

> "Anyone exercising any function under this section shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement."[45]

The Act takes in consideration the right to privacy in the general sense and not specifically the data protection. The Act however in Section 22 recognises the offence of identity theft and impersonation. The act regards identity theft as "the stealing of somebody else personal information to obtain goods and services through electronic based transactions;"[46] The act also describes "Phishing" as "the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through emails or instant messaging either in form of an email from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user;"[47] These offences involve obtaining and misusing personal data to commit some kind of fraudulent acts which is a major aspect of data protection. The act also recognises the bank's Know Your Customer Principle.[48] As earlier stated, the biggest problem with the Cybercrimes Act in relation to data protection is that the act is not a data

protection instrument *strictocensu*. Instead, the act solely addresses data protection when it crosses part with cybercrimes leaving a whole lot of other areas that need legislative cover without one. The act however takes care of some offences which are not only cybercrimes but also financial crimes. This is the extent of the relevance of the act to the banking sector. Therefore, although the act covers some aspects of data protection, such cover is not enough and unable to cater to the general data protection requirements of the country and specifically the protection of data privacy in the banking sector.

THE NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA) DATA PROTECTION GUIDELINES 2019

NITDA, being the national authority, has the responsibility of "planning, developing and promoting the use of information technology in Nigeria." It also issued guidelines on data protection (the "NITDA Guidelines"). The NITDA Guidelines provides for the minimum data protection requirements for the purpose of collecting, storing, processing, managing, operating, and technically controlling information. At the moment, the Guidelines contain detailed provisions on how personal data is stored, transferred, protected and treated. Its provisions also apply to agencies and institutions on federal, state and local government.[49]It is also applicable to private institutions that own, deploy and use information systems in Nigeria.[50]It also regulates foreign organisations that process personal data of Nigerians living abroad. The guidelines also apply to banks.

Personal data, in the NITDA Guidelines, is defined as "any information relating to an identified or identifiable natural person ("data subject") whether it relates to his or her private, professional or public life. It includes any information which can be used to differentiate or trace an individual's identity, such as names, addresses, photographs, email address, bank details, social networking details, medical information or computer IP address."[51] It includes information such as a name, address, a photo, bank details, an e-mail address, medical information, posts on social networking websites, and other unique identifiers such as, but not limited to, a MAC address, IP address, IMSI number, SIM and so on. In the guideline, data controller, is defined "as the person or entity who, whether alone or in collaboration with another, determines the purposes and means of processing personal data. Generally speaking, the organisation which collects personal data is the Data Controller. "However, Data subject is defined "as an identifiable person or one who can be identified directly or indirectly by reference to an identification factor." It must be stated that the Guidelines envisage that only natural persons can be regarded as data subjects. This is the reason why the guidelines describe processing of Personal Data as "any operation which is performed on personal data. It includes collecting, recording, organising, storage, adapting, retrieving, consulting, transmission, dissemination of data. In practical terms, every way in which an organisation handles personal data amounts to processing."

In the same vein, Sensitive Personal Data is described to include "data concerning religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, and criminal records."There are strict conditions that are attached to these types of data as they are treated as special. Private companies need not comply with the provisions of the guidelines as the provisions are merely persuasive. It is used as a point of reference by data collectors in respect of the requirements for data protection relating to collection, storage, processing, management, operation, and technical controls of personal data. In the same token, Data controllers must prevent transfer of data that does not prevent any data transfer to a country that does not meet the minimum protection of data level expected by the guidelines.[52]The NITDA Guidelines also provides that in order to determine the protection level of a country with regard to data transfer, recourse must be had to the data nature, the object and period of the proposed processing operation(s), general and sectorial rules of law that is in force in the receiving country in question. The last segment of the Draft Guidelines contains principles that underline the Data Protection Guidelines. The provisions are: "1: Personal data must be processed fairly and lawfully;[53]2: Personal Data should be used only in accordance with the purpose for which it was collected;3: Personal data must be adequate, relevant and not excessive;4: Personal data must be accurate and where necessary kept up to date; [54]5: Personal data must be kept for no longer than is necessary;[55]6: Personal data musts be processed in accordance with the rights of data subjects;7: Appropriate technical and organisational measures must be established to protect the data;[56]8: Personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection."[57]

The above principles have general acceptance as a foundation legislations relating to data protection.[58]These principles are firmly enshrined in the guidelines and legislations of many countries such as South Africa, Malaysia, and India. These guidelines must be made available to the public within three months of its adoption.[59]Some officers like Data Security Officer should be protected in order to ensure compliance with the regulations.[60]Also, policy statement on data protection needs to be developed and staff ought to be trained on data handling techniques.[61]Detailed audit of data protection practices and privacy issued also need to be conducted within six (6) months of the guideline.[62]

A CRITICAL ANALYSIS OF THE NITDA DATA PROTECTION GUIDELINES

With the coming into effect of the Data Protection Guidelines, NITDA has acted in pending when the National Assembly will deem it fit to pass legislations in this respect. Nonetheless, this cannot be equated with legislation on data protection. A careful perusal of the guidelines does not show clear legislative seriousness or creativity. It is poorly drafted. It appears like a work hurriedly drafted. Also, there is no serious enforcement mechanism stated in the guidelines. This is against world best practices.[63]Many advanced economies have serious mechanisms for data protection.[64]Nevertheless, NITDA is empowered by the guidelines to put in place Administrative Redress Panel that will receive allegations from Data Subjects; conduct investigation into the allegations; where required, issue administrative orders; and come up with apt redress.[65] This panel is no more than a quasi-judicial panel. It is not as independent as supervisory agency that can monitor the correctness of the guidelines' application. It is therefore a grave omission not to provide for specific institutional framework that will ensure adequate enforcement of data protection guidelines. More so, since NITDA does not arrogate to itself the power to enforce the guidelines, the chances of abuse of data are huge, particularly in countries like Nigeria.

Also, in spite of the replica of some major provisions in the GDPR in terms of how to handle personal data for some specific businesses in the guidelines, the regulation is not comprehensive. Some material details have been left out. This can be seen in terms of whether the data protection provisions apply to all residents, and the extent to which agencies are obliged to enforce the provisions as well as the time frame for enforcement of the guidelines. The Regulation ought to come into force when it is signed by the NITDA Board. Since it was issued on January 28, 2019, companies were asked to comply with its provisions from the date. This shows a considerable departure from the GDPR which required a two-year period for member states of the EU to conform to it.[66] Nonetheless, it can be said the regulation, being a remarkable improvement from the earlier practices, will enhance healthy business practices to Nigerians who transact businesses with the EU or its entities. Also, with the familiarity of stakeholders with the Regulation, implementation of the Data Protection Bill, currently before the National Assembly, will be smooth-sailing if it is finally enacted into law.

CENTRAL BANK OF NIGERIA'S CONSUMER PROTECTION FRAMEWORK 2016

In order to promote stable financial system in the country, being its core mandate, the Central Bank of Nigeria (CBN) developed Consumer Protection Framework (CPF). This, it is believed, will stimulate public confidence in the Nigeria's financial system. This was disclosed on November 7, 2016 for the benefits of Nigeria's consumers of financial services. The CPF has nine (9) main principles such as financial education, responsible business conduct, fairness, adequate disclosure and transparency, competition, protection of data, assets, and privacy, effective legal and regulatory structures, complaint handling/ redress and enforcement procedures[67]. The objectives of the framework are, "to guarantee high standards for efficient customer service delivery, market discipline and ensure that consumers are treated fairly by financial institutions regulated by the CBN". Financial institutions are obliged under section 6 (2) of this subsidiary legislation to keep the customers' financial activities with them private and confidential. They are also obliged to train and retrain their staff and put in place effective data protection measures that will prevent unauthorised "access, alteration, disclosure, accidental loss or destruction of customer data." They must also seek and obtain written consent of consumers before sharing their data to third parties or used for the purpose of advertisement. These principles will serve as potent checks on the activities of financial institutions in dealing with the customer data in their possession. Consumers must be accurately

and timely educated and well informed of financial products and free choice of products.

NIGERIA BANKING INDUSTRY IT STANDARDS BLUEPRINT 2015

This blueprint is not a guideline or regulatory document in the real sense. It only offers a set of standards for the application of information technology to the banking sector. One of the standards is big data. The blueprint describes big data as being described by the remarkable volumes, types and rates of data being generated by many sources, partners, customers, and regulators. Many Banks that have the capacity to harness big data, by way of customer service records, correspondence, real-time market feeds, and social media posts, may now get more useful insights into business to their competitive advantage. The objective of big data is to strengthen banking institutions in order to understand and get its customers details. The blueprint provides that where big data is successfully harnessed, it can assist banks in achieving three key objectives in transforming the banks: "Create a customer-focused enterprise; optimize enterprise risk management; Increase flexibility and streamline operations."

More so, big data allows banks to adequately understand their customers at a grittier level anticipate what customers' needs and swiftly deliver on target. This will ultimately improve the profits, retention and satisfaction of customers. This will lead to better efficiency, reduce operating costs and prevent many anticipated problems. From the wordings of the document, the blueprint seems to be more like an explanatory document rather than a regulatory document. It does not provide guidelines that must be followed or sanctions for breaching those guidelines. It simply explains the potential inherent in big data that banks can exploit to provide better service for the customers. It also states the positive implications and the risks associated with big data.

GUIDELINES ON ELECTRONIC BANKING IN NIGERIA, AUGUST 2003

In August 2003, as a result of the findings and recommendations of Technical Committee on e-Banking, the guidelines on E-banking were issued. It includes categories: "Information and Communications Technology (ICT) standards which is meant to resolves issues connected with technology solutions deployed, and to ensure that consumers' needs are met. It is also to ensure that the economy is viable and international best practice "in the areas of communication, hardware, software and security, monetary policy are promoted. This will ultimately address issues connected with how monetary policies of the CBN will be affected by the increasing usage of internet banking and electronic payments. It also includes legal guidelines to address issues relating to customer protection and to regulate issues, though generally typical to payments system, may be enlarged by electronic media use.

Strictly speaking, it can be said that the guidelines are not to protect data per se. Yet, there are data protection provisions therein. Banks are obliged to keep and maintain privacy and confidentiality of customer's bank accounts. It therefore means that banks should set up adequate risk control measures for proper risk management.[68]Also, banks must respect the customers' privacy data by using the data for only purpose for which it was meant.[69]Customers should also be permitted to decline any offer which is meant to share their data with a third party.[70]

LEGISLATIONS ON DATA PRIVACY PROTECTION

Despites series of opportunities for the law and policy makers to put in place legislations that will address the array of challenges militating against the proper usage of personal date in Nigeria, such opportunities are yet to materialize. Though there are related bills, specific ones on personal data protection are yet to see the light of the day.[71]The draft bills yet to become law are the Cyber Security and Data Protection Agency Bill[72], the Privacy Bill;[73] the Data Protection Bill,[74] the Personal Information and Data Protection Bill and the Protection of Personal Information Bill.[75] Of all the bills, the Protection of Personal Information Bill appears to be well drafted. The bill, if eventually enacted into law, will protect personal information being processed by public and private institutions. It will also initiate information protection principles in order to create minimum level of requirements for the using of individual personal information. The bill will also create an information protection regulator that will issue and regulate codes of conduct. It will also limit unsolicited or disturbing electronic communications as well as automated decision making. The purpose of this bill as contained in the preamble and long title "is to give effect to the constitutional right to privacy, by safeguarding personal information

when processed by a responsible party, to regulate the manner in which personal information may be processed, by establishing principles, in harmony with international standards, that prescribe the minimum threshold requirements for lawful processing of personal information, to provide persons with rights and remedies to protect their personal information from processing that is not in line with this Act; and to establish voluntary and compulsory measures, including an Information Protection Regulator, to ensure respect for and to promote, enforce and fulfill the rights protected by this Act."

IMPEDIMENTS TO THE ADEQUATE PROTECTION OF DATA PRIVACY IN THE NIGERIA

While it is important to analyse the present framework for the protection of data privacy, it is just as important to look into the loopholes and the problems plaguing the adequate protection of data privacy especially within the banking sector. These impediments are:

COMMITMENT LEVEL OF THE GOVERNMENT

Many countries of the world have keyed into data protection legislations. About 108 countries have legislations which partially or totally protect data.[76]Nevertheless, it means that about 30% of countries do not have such laws in place. Nigeria, the supposed giant of Africa, is part of the 30%. This implies that personal data do not receive adequate protection in these countries. Consequently, level of trust and confidence in the countries' economic activities is reduced. As earlier stated, the bills are yet to become laws in Nigeria. At continental level, in 2014, the African Union adopted Convention on Cyber Security and Personal Data protection. Not many African countries are signatories to it. In fact, only ten countries (Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia) are signatories and only two (Mauritius and Senegal) have ratified the convention. Nigeria has not yet adopted nor ratified the Convention. Also, the government normally appears suspicious of policies that seek to promote rights of individual to data privacy. This is clear in the reluctance of the government to enact the Freedom of Information Act. All these are important to show that the commitment level of the government to data privacy protection is weak in Nigeria. As such, this impedes the adequate data privacy protection in Nigeria.

NIGERIA'S HUMAN RIGHT TRACK RECORD

The Nigerian Constitution in Chapter IV specifically provides for fundamental human rights. Most of the provisions of civil and political rights are provided for in this chapter. The rights rage from right to life, right to dignity of human person, right to personal liberty, right to fair hearing, right to private and family life and so on. In fact, Chapter II of the Constitution also provides for social, economic and cultural rights by way of the fundamental objectives and the directive principles of state policies. The guidelines for the enforcement of these rights are also provided for in the Fundamental Rights Enforcement Procedure Rules. Despite these constitutional and institutional frameworks, there still persists endemic violation of human rights by the law enforcement agents. The human rights record is poor. It is difficult to bring perpetrators to book as a result of myriads of challenges facing the judicial system. At the moment, the courts are on strike as a result of lack of financial independence of the judiciary despite the constitutional guarantee of judicial independence. Rule of law is seriously being abused.[77] The right to privacy or data privacy is not an exception and it will be affected by the general apathy towards other human rights in Nigeria.

TECHNOLOGICAL AND INFRASTRUCTURAL IMPEDIMENTS

Information and Communication Technology (ICT), and engineering have over the years taken the centre stage in development. It is one of the main indicators of development in any institution or country. Currently, technological innovations impact almost every aspect of human endeavour for instance in healthcare service delivery, housing, communication, transport, banking and finance, housing, entertainment etc. while there may not be a direct link between technological impediments and the inadequate protection of human rights. There is however a level of consciousness that comes with technological penetration within a state. There is a general low consciousness of threats of personal data proliferation because of the low level of technological exposure. With the increase in the technological penetration into the banking sector, policy makers, key players in the sector now see the need to protect customer personal data.

THE AFRICAN APPROACH TO PRIVACY

Culture cannot be completely separated from the concept of privacy as it affects the general attitude of a state to the right to privacy. One of the major differences between the western and the African approach to privacy is culture. While the western society is typically individualistic; seeking ways to promote the rights of individuals, the African society is more communalistic in the sense that it seeks ways to protect the bonds that hold the community together[78]. Some authors have stated that one of the obstacles to the suitable and effective privacy protection in Africa and especially Nigeria is the predominance of the African culture of collectivism as different to the culture of individualism common in the West.[79]So, the authors opine that since Africans form a lot of associations, an individual does not really have space to claim his or her right to privacy. That is to say, individualism is an important pre-condition for the proper exercise of privacy attitudes and values. This is however foreign to the African culture; despite the fact that even within Africa, Nigeria has its own peculiarities, the culture of communalism appears to be common to all. It is however important to note that the traditional African society is gradually giving way to a modern society where privacy concerns are becoming better appreciated by a community of people with an individualistic rather than communalistic mind set.

THE LEGAL FRAMEWORK FOR DATA PRIVACY

Current state of the legal framework is one of the biggest hindrances to the protection of data privacy in Nigeria. Nigeria does not have a comprehensive (omnibus) Data protection instrument. There are a handful of regulations and guidelines like the NITDA guidelines and the various regulations released by the CBN instruments with few data protection provisions like the Cybercrimes Act. These regulations are however not enough to meet up with the complexities of data protection. Although adequate protection of data privacy goes beyond enacting comprehensive data protection legislation, it would go a long way to create a solid background, base and foundation for the protection of data privacy in Nigeria. With particular reference to the financial sector, a sector specific legislation like the Gram Leach Billey Act[80] in the United States of America would help to also reduce the impediments to the adequate protection of data privacy in the Nigerian banking sector.

TOWARDS LEGAL REFORMS

This paper shows that not much has been done in protecting personal data in Nigeria. Yet, policy makers seem to underplay the dangers posed as a result of the paucity of legal framework on data protection. Legal reforms on data protection will redeem the gloomy nature of the prospects for the future on data protection. Government's attention needs to be seriously drawn towards the challenges of personal data explosion. Several lessons can be drawn from the legal reforms put in place by other comparable countries, especially in Africa. Nevertheless, some practical measures need to be put in place for a more successful and effective legal reform on personal data protection in Nigeria. First, data protection needs to be given adequate priority. A problem identified is close to being tackled. Therefore, a better understanding of the need to regulate personal data processing by policy makers with appropriate legal regime is fundamental for control of data protection to work efficiently. Likewise, of particular interest in this perspective is the level of awareness of the people because the more the people know about the dangers of uncontrolled private data processing, the more they seem to care. This is in view of the fact that data protection as a subject raises fundamental issues that transcend the conventional understanding of the right to private life. Furthermore, the absence of Data Protection Agency is an issue that must be taken with all seriousness for an effective legal regime. Though there is Human Rights Commission in existence; however, the powers and scope of this Commission to address data protection issue is minimal for the obvious reason that the Commission was established at a time when the protection of private data was never contemplated. Secondly, there is no denying that data protection has its origin in the right to privacy as stipulated in the international human rights documents such as the Universal Declaration of Human Rights (UDHR), [81]International Covenant on Civil and Political Rights (ICCPR),[82] African Charter on Human and Peoples' Rights and European Convention on Human Rights (ECHR).[83] Therefore, the root of data protection is in human rights instruments which perhaps make it a human right as well. Though some countries seem not to distinguish privacy from data protection and as such, the right to data protection has been interpreted to be

embedded in the right to privacy. However, rather than recognize data protection as part of the right to privacy, there is an emerging trend to data protection as a separate human right. For instance, under the EU legal order, data protection is now seen as an autonomous human right and the EU Charter has separated data protection from the right to privacy. In addition, some countries have included the right to data protection in their Constitution in order to give it a constitutional flavour.[84] While the right to privacy and the right to data protection seems to be similar, their qualitative contents and what they seek to protect and achieve are not the same. The right to privacy does not adequately cover the right to data protection. There is the need to recognise data protection as a human rights issue that must be given priority. Therefore, to effectively tackle the data protection issue in Nigeria, there is a need to amend the Constitution of the Federal Republic of Nigeria to incorporate data protection as a human right. By so doing, it will elevate data protection to the same level as other rights contained in the Constitution. Finally, due to the trans-border nature of data protection, it is time for Nigeria Government to demonstrate serious commitments to its obligations under regional and sub-regional instruments on data protection. For instance, there is the need to start working on the ratification of the AU Convention on Cyber Security and Data Protection within the shortest possible period. While it is true that there are some gaps in this Convention, it could be an eye opener in the right direction in realizing the right to data protection in Nigeria. Likewise, it is expected that Nigeria must honour its obligations under the ECOWAS Supplementary Act on Data Protection that legally binding since it is an integral part of the ECOWAS Treaty. Since both regional instruments are mostly stirred by the EU framework, they may perhaps offer some guidance towards effective legal regime on data protection in Nigeria.

CONCLUSION

From the foregoing analysis, legal architecture on data protection in Nigeria is weak and ineffective in stemming the tide of the challenges posed by data challenges. Consequently, effective legal framework on data protection is necessary for the enjoyment of the opportunities of this digital age. This is because data privacy rights and bankers' business interests are two important components necessary for the development of the already fragile nation's economy. Although there are several guidelines and laws that currently make up the legal framework of data privacy within the Nigerian banking section and which seek to sustain the bankers' business interests, they do not provide adequate protection for the kind of sensitive personal data processed within the sector. In addition, the present bills in the legislature need to be worked upon and fine-tuned to meet the data protection requirements of the country in the banking sector without affecting the legitimate business interests of bankers. In this paper, an attempt has been made to dissect and analyse the legal framework for the protection of data privacy especially within the banking sector. This was done by examining the constitutional provision on the right to privacy, its bearing on and its relationship with the right to data protection. Furthermore, the current legislative framework on data privacy in the banking sector was analysed. In doing this, the paper examined at the Credit Reporting Act and the Cybercrimes Act. A critical analysis was also carried out into the 2019 NITDA Guidelines in order to gauge its level of adequacy as to data protection and its level of compliance with the GDPR. Sector specific regulations on data protection within the banking sector were also analysed and it was discovered that they still do not provide adequate protection for customer personal data in the banking sector especially in comparison to the nature of sensitive personal data processed within the sector. The paper likewise analysed the CBN and NITDA and the roles they play in protecting personal data and information within the banking sector. Several legislative attempts have been made towards data Protection; none of these Bills has however been passed by the legislature and none of them borders on the banking sector specifically. Finally, the various impediments to the adequate protection of data privacy in Nigeria were examined. It is therefore suggested that effective data protection legislation in Nigeria particularly in the banking sector would protect data privacy as well as the legitimate business interests of bankers in Nigeria.

NOTES

1 The Economist, The World's Most Valuable Resource Is No Longer Oil, But Data, May 6th, 2017, available at https://www.google.com/amp.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data 2018

2 Robinson N. Review of the European Data privacy Directive (Technical report), RAND Corporation (May 2009), available at http://www.rand.org.pubs/techical_reports/TR710.html 2018

[3] Zulhuda Sonny, Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks, South East Asia *Journal of Contemporary Business, Economics and Law,8(4), 1-6, 2015.*

[4] International instruments that recognize this right include the UDHR, ECHR, ACPHR etc.

[5] Namely Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia and Western Sahara.

[6] Rich C. Privacy Laws in Africa and the Near East, *6 Bloomberg BNA World Data privacy Report*, 1, (2016)

[7] Shroff M., Nehriya N. and Vasan V. Privacy in the banking sector: striking a balance, 2017 http://bankingfrontiers.com/data-privacy-banking-sectorstriking-balance 2018

[8] Olusegun A.S, Ishola G.K. & Hammed A.B., Effect of Electronic Banking on Employees' Job security in Nigeria, *European Journal of Humanities and Social Sciences*, 4(2), 69-84, 2011.

[9] CBN launched the Bank verification Number (BVN) project in February 2014. According to the CBN, the objective of the project is to protect bank customers, reduce fraud and further strengthen the Nigerian banking system.

[10] Bygrave L.A., Privacy and Data Protection in an International Perspective, Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010, available at www.scandinavianlaw.se/ 2019

[11] Bygrave, L.A., Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague / London / New York 2002, chapter 7.

[12] Cited in Bygrave, L.A., Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague / London / New York 2002, chapter 7.

[13] Akinsuyi F.F. Data Protection Legislation for Nigeria: The Time is Near, *Economic and Policy Review*, 13(3), 31-39, 2007

[14] Bygrave L.A, 'Data Protection Law: Approaching Its Rationale, Logic and Limits', Kluwer Law International, The Hague/London/New York 2002, 1.

[15] Cuijpers C, A Private Law Approach to Privacy: Mandatory Law Obliged? *Scripted*, 312, 2007.

[16] De Hert P. and Schreuders E., The Relevance of Convention, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19–20 November 2001.

[17] . See Article 8 of the EU Charter of Fundamental Rights, 2001.

[18] The Economist, The World's Most Valuable Resource Is No Longer Oil, But Data, May 6th, 2017, available at https://www.google.com/amp.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data 2018

[19] CBN exercises, inter alia, regulatory oversight functions over by banks and other financial institutions in Nigeria.

[20] Para. 3.21 of the CBN Guidelines for Card Issuance and Usage.

[21] Para. 3.22 of the CBN Guidelines for Card issuance and Usage.

[22] 'How KYC determines your banking relationship' The Punch, 14 Sep 2018 available at https://www.pressreader.com

[23] Ebije 1.A., BVN and Nigeria's Data Management Malaise, *People's Daily Newspaper*, 23, 2015.

[24] Taiwo I. Things That Could Go Wrong With The BVN, Which No One Is Talking About, 2015 https://techcabal.com/2015/11/03/things-that-could-go-wrong-with-the-bvn-which-no-one-is-talking about

[25] Report of The Technical Committee on Electronic Banking, February 2003.

[26] Dawson, T., 'The Role of Security, Privacy, Usability and Reputation in the Development of Online Banking, *Online Information Review*, 31(5) 583-602, 1998.

[27] Olusegun A.S, Ishola G.K. & Hammed A.B., Effect of Electronic Banking on Employees' Job security in Nigeria, *European Journal of Humanities and Social Sciences*, 4(2), 69-84, 2011.

[28] Ololade B and Ogbeide S., E- Banking in Nigeria: Issues and Challenges, *Research Journal of Finance and Accounting*, 8(6), p.16, 2017

[29] KutiF,, Obi U. and Azubuike S., The Privacy, Data Protection and Cyber security, *Law Review* p. 247, 2017.

[30] The Bills relate to collection of and protection of personal information or data and makes provisions for a Privacy Commissioner to address violations under the provisions of the proposed legislation. Unfortunately, there are no specific references to electronic surveillance of privacy rights contained therein.

[31] Onwuegbuchi C. 'CBN Mandates Banks' Directors to Protect Data', Nigeria Communications Week, 2018 available at https://nigeriacommunicationsweek.com.ng/cbn-mandates-banks-directors-to-protect-data

[32] Section 1 of the Credit Reporting Act 2017

[33] Ibid, Section 2

[34] Section 9 (1)

[35] Section 9 (2) (b) (ii)

[36] Section 9 (2) (b) (i)

[37] Section 27

[38] Section 3 (1) (a) and (b)

[39] Section 3 (b)

[40] Section 6 (1) and Section 12 (a)

[41] Section 3(b)

[42] Section 3 (d)

[43] Section 7 (1) and (2) (l)

[44] Section 1 (c) 0f the Cybercrimes Act 2015

[45] Section 38 (5) Cybercrimes Act 2015

[46] Section 22 (b) and 59 cybercrimes Act 2

[47] Section 59 of the Act

[48] Section 37 of the Act

[49] Section 1.3

[50] Section 1.4

[51] Section 1.3 of the Guidelines

[52] Sec 2.11 of the guidelines

[53] Section 2.2

[54] Section 2.1 (1) (b)

[55] 2.1 (1) (c)

[56] Section 2.1 (1) (d)

[57] Section 2.11 and 2.12

[58] Dr.Jemilohun B.O and Prof. AkomoledeT.I , Regulations or Legislation for Data Protection in Nigeria? A Call for a Clear Legislative Framework, *Global Journal of Politics and Law Research*, 3(4), p.1-16, 2015.

[59] Section 4.1 (1).

[60] Section 4.1 (2).

[61] Section 4.1 (3)

[62] Section 4.1 (5)

[63] Ibid at 29.

64 The European Union Data Protection Directive now replaced by the GDPR in Article 28 mandates each member state to create an independent supervisory agency to monitor the application of data protection laws and to investigate violations

65 Section 4.2 of the NITDA Data Protection Regulation

66 Dr.Jemilohun B.O and Prof. AkomoledeT.I , Regulations or Legislation for Data Protection in Nigeria? A Call for a Clear Legislative Framework, *Global Journal of Politics and Law Research*, 3(4), p.1-16, 2015.

67 Salau O., The CBN Issues Its Consumer Protection Framework, available at http://www.odujinrinadefulu.com/content/cbn-issues-its-consumer-protection-framework 2019

68 Section 3.0 (c) of The Guidelines.

69 Section 3.0 (d) of The Guidelines.

70 Section .1 of The Guidelines

71 See for example the Computer Security and Critical Information Infrastructure Protection Bill (2005); Cyber Security and Data Protection Agency Bill 2008; Electronic Fraud Prohibition Bill 2008. In 2009, there was the Computer Security and Protection Agency Bill and Computer Misuse Bill. Then the Economic and Financial Crimes Commission Act (Amendment) Bill 2010 and the Cyber Security and Information Protection Agency Bill 2012. These entire draft bills have provisions related to data protection.

72 Available at http://www.nassnig.org/nass2/legislation.php?id=410accessed on 3 March 2019

73 Available at http://www.nassnig.org/nass2/legislation2.php?search=privacy&Submit=Searchaccessed on 3 March 2019

74 http://www.nassnig.org/nass2/legislation2.php?search=data+protection&Submit=Searchaccessed on 3 March 2019

75 Kio-Lawson T., 'Right to be Forgotten', Business, available at http://businessdayonline.com/2014/06/right-to-be-forgotten/#.VF5UKjTF9yJ 2019

76 UNCTAD, Global cyber law tracker, available at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eComGlobal-Legislation.aspx 2019

77 Onwuazombe I.I., Human Rights Abuse and Violations in Nigeria: A Case Study of the Oil-Producing Communities in the Niger Delta Region, 22(1) p.8, *Annual Survey of International & Comparative Law*, 2017

78 Bakibinga E.M., Managing Electronic Privacy in the Telecommunications Sub-Sector: The Ugandan Perspective, available at http//:thepublicvoic.org/eventscapetown04/bakibinga.doc 2019

79 Bygrave L.A., Privacy and Data Protection in an International Perspective, *Scandinavian Studies in Law*, 56, 165–200, 2010.

80 Also called the Financial Services Modernization Act of 1999

81 UDHR, Article 12

82 ICCPR, Article 17.

83 ECHR, Article 8. The African Charter on Human and Peoples" Rights (ACHPR), unfortunately, does not contain a right to privacy.

84 Example, Belgian Constitution (1831), Article 22; Portuguese Constitution (1976), Article 26; Spanish Constitution (1978); Article 18 and Swedish Constitution (1975), Article 2. In other countries like Canada, data protection is a quasi-constitutional right. See the decision of the Canadian Supreme Court in H.J. Heinz and Co. Ltd v. Canada (Attorney General), [2006] SCC 13, para. 28.

REFERENCES

Akinsuyi, F. F. 2007. Data protection legislation for Nigeria: The time is near. *Economic and Policy Review* 13(3): 31-39.

Bakibinga, E. M. 2019. Managing electronic privacy in the telecommunications sub-sector: The Ugandan perspective. http//:thepublicvoic.org/eventscapetown04/bakibinga.doc [[7 May 2019].

Bygrave, L. A. 2010. Privacy and data protection in an international perspective. *Scandinavian Studies in Law* 56: 165–200.

Bygrave, L.A. 2002. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Kluwer Law International.

Cuijpers, C. 2007. A private law approach to privacy: Mandatory law obliged? *Scripted* 312.

Dawson, T. 1998. The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review* 31(5): 583-602.

De Hert, P. and Schreuders, E. 2001. The Relevance of Convention, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19–20 November 2001.

Ebije, 1.A., 2015. BVN and Nigeria's data management malaise. *People's Daily Newspaper*, 23.

Jemilohun, B. O. and Akomolede, T. I. 2015. Regulations or legislation for data protection in Nigeria? A call for a clear legislative framework. *Global Journal of Politics and Law Research* 3(4): 1-16.

Kio-Lawson T. 2019. Right to be forgotten. http://businessdayonline.com/2014/06/right-to-be-forgotten/#.VF5UKjTF9yJ [7 May 2019]

Kusamotu, A. 2007. Privacy law and technology in Nigeria: The legal framework will not meet the test of Adequacy as Mandated by Article 25 of European Union Directive 95/46, 16/2 *Information & Communications Technology Law*: 149–59.

Kuti, F., Obi, U. and Azubuike, S. 2017. The privacy, data protection and cyber security. *Law Review* 247.

Ololade, B. and Ogbeide, S. 2017. e-banking in Nigeria: Issues and challenges. *Research Journal of Finance and Accounting* 8(6): 16.

Olusegun, A. S., Ishola, G. K. & Hammed, A. B. 2011. Effect of electronic banking on employees' job security in Nigeria. *European Journal of Humanities and Social Sciences* 4(2): 69-84.

Onwuazombe, I. I. 2017. Human rights abuse and violations in Nigeria: A case study of the oil-producing communities in the Niger Delta Region. *Annual Survey of International & Comparative Law* 22(1): 8.

Onwuegbuchi, C. 2018. CBN mandates banks' directors to protect data. Nigeria Communications Week, https://nigeriacommunicationsweek.com.ng/cbn-mandates-banks-directors-to-protect-data

Rich, C. 2016. Privacy laws in Africa and the near east. *6 Bloomberg BNA World Data privacy Report*, 1.

Robinson N. 2009. Review of the European Data privacy Directive (Technical report), RAND Corporation, http://www.rand.org.pubs/techical_reports/TR710.html [15 November 2018].

Salau, O. 2019. The CBN Issues Its Consumer Protection Framework http://www.odujinrinadefulu.com/content/cbn-issues-its-consumer-protection-framework [16 October 2019]

Shroff, M., Nehriya, N. and Vasan, V. 2017. Privacy in the banking sector: Striking a balance. http://bankingfrontiers.com/data-privacy-banking-sectorstriking-balance [7 May 2018]

Taiwo, I. 2015. Things that could go wrong with the BVN, which no one is talking about. https://techcabal.com/2015/11/03/things-that-could-go-wrong-with-the-bvn-which-no-one-is-talking about [6 February 2019]

UNCTAD. 2019. Global cyber law tracker. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eComGlobal-Legislation.aspx [7 May 2019]

Zulhuda Sonny. 2015. Data breach on the critical information infrastructures: Lessons from the wikileaks. *South East Asia Journal of Contemporary Business, Economics and Law* 8(4): 16.

Abdulkadir Bolaji Abdulkadir
Department of Public Law
Faculty of Law
University of Ilorin
Nigeria
Email: abdulkadir.ba@unilorin.edu.ng

Abdulfatai Oladapo Sambo
Department of Public Law
Faculty of Law
University of Ilorin
Nigeria
Email: fataisambo@yahoo.com