A SURVEY OF THE NIGERIAN PERSONAL DATA AND PRIVACY PROTECTION LAWS*

Abstract
Global indices show that Nigeria has grown tremendously over the years in technology adoption which thrives on collection, processing, storage and transmission of huge amounts of citizens' data. However, the absence of robust legal and institutional frameworks in the country that address the crises and disputes arising from electronic data processing is exacerbating concerns of trust and confidence among technology users in Nigeria. This is so even in the presence of fragments of data protection legislations. Consequently, this chapter analysed the existing fragments of data protection and privacy laws and regulations in Nigeria, causes and consequences of data breaches, challenges of developing data protection legislations in developing countries, identified gaps in the existing laws and proffer recommendations for a principal data privacy and protection legislation and establishment of a data protection authority that will drive the implementation of the principal data protection laws.

Keywords: Confidentiality, Principal, Legislation, Data, Protection.

1. Introduction

A wide range of socio-economic and political activities are moving online, adopting various information and communications technology options that have a transformational impact on the way business is conducted; the means by which people interact among themselves, with government, enterprises and other stakeholders in the digital society. Essentially, humanity is migrating to the cyberspace thus, giving rise to new business models and a variety of innovations. Data is at the centre of this entire scheme, as it is referred to now as the new currency[1]. Consequently, data has become the most priced commodity in the e-economy as everything else have been dematerialised from their physical forms to digitized data. For example, money which was in the past carried about in paper or coin forms is now largely digitized, held and transferred on computing infrastructure across the globe with tremendous ease in physical efforts and financial cost; giving rise to buzz phrases like 'cashless economy', 'paperless office', etc. Other aspects of human endeavours have equally witnessed similar transformation. Thus, nations, organisations and individuals seek to adopt more technology into their everyday activities so as to continuously and increasingly harness the associated gains of the connected society. In Nigeria, there have been tremendous efforts by government through the National Information Technology Development Agency (NITDA) to adopt e-governance at the various levels of the governance structure.[2] This implies that government agencies will routinely collect, store and exchange confidential and personal information of data subjects with individuals and business organizations across the technology ecosystem. This is evident in the United Nations E-Government Development Index (EGDI) reports for the past years ((E-Government Development Index, 2012-2018), the International Telecommunications Union (ITU) ICT Development Index (IDI) (International Telecommunications Union, 2018) and the World Economic Forum (WEF) Network Readiness Index (NRI) (Word Economic Forum, 2016). Nigeria has slowly but continuously increased her score and ranking in these indices and promises to soar even higher. The private sector is witnessing even more technology adoption ostensibly to tap from the enormous advantages of technology driven enterprises. This evident growing consumption of ICT by government, private enterprises and individuals is largely driven by personal data. For instance, in recent years, the Nigerian government is driving the national identification scheme through the National Identity Management Commission (NIMC), this is generating a huge national database of individuals that contains virtually every detail that can lead to identification of natural persons, these data are collected and held electronically. The electoral body, the Independent National Electoral Commission (INEC) holds similar data on individuals of voting age. The telecoms services providers on the orders of the regulator, the National Communications Commission (NCC) collects through third parties, stores and process data of natural persons who subscribes to their services; similarly, commercial banks under the instructions of the Central Bank of Nigeria (CBN) build a huge harmonised database of bank customers through the bank verification number (BVN). Every government scheme in recent times requires the collection and processing of personal data. In the private sector, local and international businesses now thrive on data; that is whether they are e-commerce centres or other forms of electronically driven businesses. From the foregoing, it is deducible that there is a plethora of

***By Habiba MUSA**, Nasarawa State University, Keffi, Nigeria; and
***Victor E. KULUGH**, Nasarawa State University, Keffi, Nigeria

[1]World Economic Forum. (2016). The Global Information Technology Report 2016. In *Insight Report*<http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf%0Ahttps://www.weforum.org/reports/the-global-information-technology-report-2016.> Retrieved from http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf%0Ahttps://www.weforum.org/reports/the-global-information-technology-report-2016>https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. Accessed 20/1/ 2022.

[2] National Information Technology Development Agency *Nigeria e-Government Interoperability Framework (Ne-GIF)* [2019] *National Information Technology Development Agency (NITDA)*on 12/11/2021.

electronically managed databases in Nigeria by either government or private concerns. However, there is no commensurate legal and institutional frameworks to address the challenges and conflicts associated or arising from the collection, storage, processing and transmission of such data, although, there exist a fragment of laws and regulations addressing some aspects of data protection in specific industry segments. This paper x-rays these laws to uncover the gaps, overlaps and proffer recommendations on the necessity of a principal data protection, privacy and confidentiality legislation that will give birth to a data privacy and protection institution. This is particularly important in an era of growing technological transformation.

2. Background

Advances in ICT have increasingly provided facilities and tools for profiling and tracing individuals using the data stored about them, also referred to as personal data; thus, making it a favourable tool for gathering and processing personal data legitimately or otherwise, with or without the consent of the data subject(s).[3] The fact that such information can be easily accessed and shared without authorization from the data subject and even used to the detriment of the owners amplifies serious concerns on the protection of personal data and privacy of data subjects. This calls for overarching national legal and institutional frameworks for the implementation of data and privacy protection regimes of personal data of individuals from eminent breaches. This position has been anchored by global, regional and sub-regional bodies such as the United Nations,[4] the African Union (AU),[5] and the Economic Community of West African States[6] (ECOWAS) through various conventions and initiatives. These bodies have severally and jointly at various times mandated their member states to develop legal and institutional frameworks for personal data and privacy protection. The ECOWAS Data Protection Act and the AU Convention on Cyber-security and Personal Data Protection (AU CCPDP) specifically mandated member states to commit themselves to developing legal and institutional frameworks for personal data and privacy protection in their respective states.[7] According to the United Nations Conference on Trade and Development (UNCTAD)[8] out of the 54 African nations, 28 have full data and privacy protection legislations, 6 are at draft stage, 9 have no legislation and there is no data about 11. The legal framework will give birth and power to independent Data and Privacy Protection Authority which will have administrative role and ensure that any data processing activity takes cognisance of the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State and the rights of local communities.[9] The realm of e-commerce and international trade is fuelled principally by personal data of individuals; most of these data is of sensitive nature thereby, increasing the importance of data protection and privacy. Data protection is directly related to trade in goods and services in the digital economy and insufficient protection can create negative market effects by reducing consumer confidence thereby, adversely affecting trade flows, especially of transborder nature that rely on technology. Besides, most social and cultural norms around the world include a respect for privacy.[10] Consequently, the presence of legal and regulatory regime in this regard will be an incentive to both local and foreign investors who would want to consider engaging in trade ventures in Nigeria.

3. Innovations and Data Protection

The geometric rise in the complexity and quantum of device interconnectedness and the data thronging through networks powered by innovations and convergence of new technologies is increasing the urgency of the need for data protection laws notwithstanding the tremendous social and economic gains globally. Innovations like the Internet of Things (IoT), bigdata analytics, cloud computing, social networks and mobile technologies have astonishingly increased the quantum, speed, accuracy and quality of data collection, analyses and dissemination while dramatically reducing the cost involved in data management. For instance, it is increasingly becoming

[3] Economic Community of West African States. (2010). *SUPPLEMENTARY ACT A1SA . 1f01f10 ON PERSONAL DATA PROTECTION WITHIN ECOWAS*. Retrieved from http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf/ on 21/12/2021.

[4] United Nations, 'Measuring the Impacts of Information and Communication Technology for Development Measuring the Impacts of Information and Communication Technology for Development' 2011 in *United Nations Conference on Trade and Development*.

[5]African Union, *African Union Convention on Cybersecurity and Data Protection* 2014<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> Accessed 21/2/2022.

[6]Economic Community of West African States, Supplementary Act AISA 2010<http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf/> Accessed 21/2/2022.

[7]AU CCPDP 2014 (n5) and ECOWAS 2010 ibid. Report accessed from <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx>Accessed 22/2/2022.

[8]United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development 2016<https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx>Accessed 21/2/2022 Accessed 22/2/2022.

[9] AU CCPDP (n7).

[10] UNCTAD 2016 and World Economic Forum 2016.

easier and cheaper to gather, process and disseminate data without any of the barriers of time and location as data which was hitherto held on hard copy files and locked up in file cabinets in offices and homes is now de-materialized and residing on storages of computing devices as well as been transmitted on electronic networks across the globe. Consequently, the value attached to these electronic data is great and varied. Access to data translate to value, therefore, motivation to illicitly have access to these data by state and non-state cyber actors and use them in a manner that is potentially harmful to the data subjects is increasingly threatening to undermine the gains of the information society. Similarly, crimes are gradually migrating to the cyberspace proportionately with the migration of legitimate human endeavours. The greatest challenge therefore, is that of ensuring the protection and privacy of data once it is transferred from a data subject to the custody of a data controller, data processor or other third parties.

Currently, there are a variety of technical options for data and privacy protection across the technology ecosystem aimed at ensuring the protection, privacy and confidentiality of data. These are however constantly violated with the attendant consequences of data breaches. Given the criticality of these data elements to netizens and by extension, organisations and nation states; it behoves on nations to provide technical and legal mechanism to prevent and respond to data breaches in a manner that restores trust and confidence in the technology economy. One best feasible alternative is for nations or states to provide legislations that will birth mechanisms capable of addressing conflicts and violations that may arise during electronic data interchange. These legislations must also be capable of synchronising with global, regional and sub-regional efforts, so as to address the transnational nature of the data protection problem. However, in Nigeria, there is presently no principal or comprehensive data privacy or protection law. What exist is a plethora of sectoral laws addressing problems within their respective sectors. Consequently, there is no data protection authority to independently provide administrative over sight on the data processing value chain.

4. The OECD Guidelines and the Fair Information Practice Principles

The Organisation for Economic Cooperation and Development (OECD) Guidelines and United States of America's fair information practices principles provide lesson for countries like Nigeria that have over the last ten years been working on a data protection bill that is still at the draft stage. The OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data were developed by OECD member states in consultation with a broad group of stakeholders. They were originally published in 1980 but were revised and re-issued in 2013.[11] The Guidelines can be followed by any country, not necessarily OECD members. Thus, they have influenced the content of privacy laws globally, beyond the OECD's member states. With their long history and creation of balance between transborder flows of personal data and data protection, they have found wide acceptability and adoption across many nations of the world. The Fair Information Practice Principles (FIPP)[12] are similar to the OECD guidelines and can also be adopted by any nation state in their data protection law making efforts to address some of the data and privacy protection concerns. The FIPP states some principles such as purpose specification, collection limitation, and use limitation. The collection of personal information should be limited, and its use should be limited to a specified purpose. Majority of the laws surveyed in Table1 did not make direct or implied reference to these baseline global principles except the NCC Consumer Code of Practice Regulation 2007, which relates its data and privacy protection principles to these important international guidelines.

5. Parties in the Data and Privacy Protection Ecosystem

For data processing activities to be carried out in such a manner that the data and privacy of data subjects is protected while preserving the prerogative of the government and local authorities, the legislation must adequately delineate the relationships and roles among the various entities that exist and interrelate within the ecosystem. Thus, the entities considered here are: the data subject, data controller, data processor, third parties, data and privacy protection authority and data and privacy protection legislation. Figure 1 defines parties in a data and privacy protection ecosystem:

[11] UNCTAD 2016.

[12]United States Government Accountability Office <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx>2008.Accessed 3/3/2022.

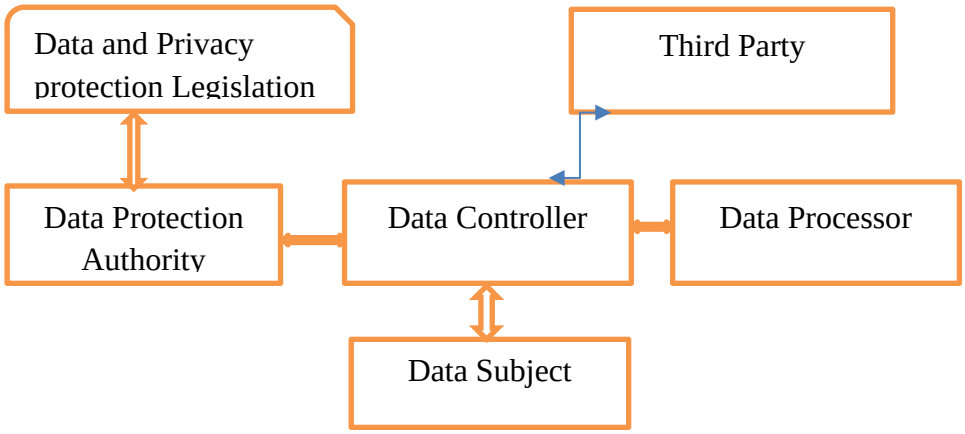

Figure 1: Parties in Data and Privacy Protection Ecosystem

Data and Privacy Protection Legislation

This is a national principal legislation that governs the operations of data protection on the data processing value chain, it is expected to synchronise with global, regional and sub-regional efforts to tackle the protection of transborder flow of data through international trade, e-commerce and even diplomatic engagements.

Data and Privacy Protection Authority

This is an independent institutional body that is given birth to and empowered by the data and privacy protection legislation to provide administrative oversight by implementing the letters of the law. That is, ensuring that personal data is processed according to the provisions of the legislation.

Data Controller

Any public or private individual or legal entity, a body corporate or association who, alone or jointly with others, decides to collect and process personal data and determine the purpose for which such data are processed.

Data Processor

Any public or private individual or legal entity, a body corporate or association who processes personal data on behalf of the data controller.

Third Party

Any public or private individual or legal entity, a body corporate or association other than the data subject, the data controller, the data processor and any other person directly placed under the authority of the data controller or data processor who is authorized to process personal data.

Data Subject

An individual who is subject of the personal data processing is a natural person whose data is been collected, processed, stored and transmitted by the other parties in the data processing arrangement. The data about him or her is referred to as personal data. When such data are capable of been used separately or jointly to identify a person, they are called personal identifiable information (PII); some PII are of sensitive nature.

Personal Identifiable Information (PII)

Data or pieces of information that are of sensitive nature which when not adequately protected may be accessed by criminally minded individuals and organisations which may identify an individual and potentially cause harm or monumental lose to their owners. Such data may include information relating to natural persons that may lead to the unveiling of their identities. PII is any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[13]

[13]E. McCallister, T. Grance, & K.A. Scarfone *Guide to protecting the confidentiality of Personally Identifiable Information (PII)* 2010<https://doi.org/10.6028/NIST.SP.800-122>Accessed 3/3/2022.

Sensitive Data

This refers to personal data relating to an individual's religious, philosophical, political, trade union opinion or activities; to his sexual life, racial origin or health, relating to social measures, proceedings, and criminal or administrative sanctions.[14]

6. Causes and Consequences of PII Breaches

The anonymity in which personal data can be accessed by unauthorised parties through the technology pathway is further fuelling the way and manner in which data and privacy of entities is violated or breached.[15] This anonymity of access is potentially harmful to the data subject since they do not know who, where, when, why and how the data accessed about them could be applied. Distributed and virtualized data collections and analysis environments have made it increasingly difficult for data subjects to have a prior knowledge of who may need access to data, when and where this may happen and whether that data could be or contain Personally Identifiable Information (PII) or sensitive data. Though most online forms have a consent component, data subjects are hardly capable of reading through to understand the contents before clicking to signal agreement with the data collection entity. Data subjects in the digital economy globally are increasingly getting concerned about what happens to the data that is collected from them, these concerns are further exacerbated with the frequent occurrence of data breaches and the absence of a clear-cut means on how and where to seek redress in the event of a breach heightens these concerns. Cumulatively, breaches lead to tremendous loss of confidence resulting to reduced data flows which will in turn harm e-commerce and other activities that are internet reliant thus reducing societal benefit. From a trade perspective, transfers of data to and from developing countries may be inhibited by an absence of domestic legal protection, with missed business opportunities as a possible result. In countries that see exports of ICT-enabled services as a promising growth sector, data protection laws are important to comply with requirements in the importing countries. However, a majority of developing countries still lack legal frameworks to secure the protection of data and privacy.[16] Consequently, Nigeria, and a host of other developing countries risks been cut-off from key international trade opportunities in the absence of a substantive and principal data and privacy law, because many trade transactions require cross-border data transfers that are subject to minimum legal requirements.

7. Challenges of Data and Privacy Protection Laws in Developing Countries

Enacting data and privacy protection legislation is the most important first step in the data and privacy protection journey. However, enacting legislations in developing countries is usually cumbersome and time consuming especially as there are usually, laid down procedures and processes pre-agreed by law through which legislations are birthed. The enactment of data and privacy protection laws in developing countries is especially encumbered by these procedures coupled with the associated financial costs and the general knowledge-gap on the part of legislators to understand the concepts and imports of the various elements of the emerging fast changing ICT legislations. The following specific challenges typically slow down the process of enacting and implementing data protection laws in developing countries:

i. Length of time, cost and legislative knowledge-gap in enacting legislation: ICT and its peculiarities are relatively new, it is also an area where multiple new innovations and business models are developed at a fast pace. Developing legislations to cope with this speed will require law makers to regularly acquaint themselves with developments as they occur in the technology sphere.
ii. Cost of implementation: Establishing and running a Data Protection Authority (DPA) may require a substantially huge budget. In a country where government is already overwhelmed by funding of agencies, an additional agency with new financial obligations in funding personnel, training and infrastructure may be difficult to bear.
iii. Skilled manpower needed to run DPAs as well as administering the entire data and privacy protection ecosystem such as technology savvy judges, lawyers, law-enforcement personnel and ICT experts are lacking, cost of training and the time it takes to train them is a major draw-back in the implementation of the data protection laws.

[14] E. McCallister et.al. European Telecommunications Standards Institute. (2018). Personally Identifiable Information. In *Encyclopedia of Social Network Analysis and Mining* (Vol. 1). https://doi.org/10.1007/978-1-4939-7131-2_100873.
[15] E. McCallister et.al.
[16]Internet Society (ISOC) & African Union, *Personal Data Protection Guidelines for Africa* 2018<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> on 25/11/2021.

8. Data and Privacy Protection Laws in Nigeria

Data and privacy protection laws are made to protect an individual also referred to as the data subject from the violation of their privacies at the different levels of data processing by the various parties involved in the data processing value chain. Nations, sub-regional, regional and global organisations have instituted legislations to provide a fair environment for processing data and build confidence in those whose data will be collected, processed, stored and transmitted. To this end, the FIPP; the OECD principles for transborder information flows;[17] the European Union General Data Protection Regulation and many other data protection conventions, charters and regulations provide guidelines on the protection of individual's data. However, these laws, regulations and principles have jurisdictional restrictions and may not be applicable for seeking legal redress in other nation states for the violation of one's privacy.

In Nigeria, there is no principal data and privacy protection law.[18] However, there are a couple of legislations addressing data protection in particular sectors, this means that there is no national data protection authority. The Constitution of the Federal Republic of Nigeria (FRN) provides for the protection of the privacy of Nigerian citizens in general terms. Section 37 of the Constitution provides that: 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.' Additionally, there are other subsidiary data protection legislations and regulations, namely; The Child Rights Act (CRA)[19] which regulates the protection of children (persons under the age of 18 years). The CRA limits access to information relating to children in certain circumstances. Section 8 of the CRA guarantees every child's entitlement to privacy, family life, home, correspondence, telephone conversation and telegraphic communications, while section 205(2) prohibits the publication of any information that will lead to the identification of a child offender, and requires that the records of child offenders be kept strictly confidential and closed to third parties except in certain limited circumstances.

The FOI Act 2011 though not a data protection law impacts on the protection of the information of individuals in Nigeria. Under section 14 of the FOI Act 2011, a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Personal information is defined as 'any official information held about an identifiable person but does not include information that bears on the public duties of public employees and officials. Section 16 of the FOI Act also provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law such as lawyer-client privilege and journalism confidentiality privilege. The Cybercrimes (Prohibition, Prevention, etc. Act 2015) criminalised the abuse and misuse of data for fraudulent purposes. Service providers have a duty of record retention and data protection. They are to keep all traffic data and subscriber information for a period of two years. The Credit Reporting Act 2017 in the financial sector, promotes access to credit information. Amongst other things, it protects the confidentiality right of data subjects, including the right to consent and right to accurate personal information. The National Health Act 2014 requires health services providers to keep records of patients' personal information by storing every user's health record safely and in strict confidentiality.

Others are regulations within specific sectors to deal with data protection as it concerns the businesses of these sectors. In this category, there is the Nigerian Data Protection Regulation, 2019 (NDPR) which was issued by the National Information Technology Development Agency (NITDA). The Nigerian Data Protection Regulation 2019 was made by virtue of the National Information Technology Development Agency Act 2007. While the NDPR is very similar to the EU-GDPR, it is not a law emanating from a legislative process. The Consumer Code of Practice Regulation (CCPR) was issued by the Nigerian Communications Commission (NCC) in 2018[20]. The CCPR provides that all licensees, that is, the telecoms service providers who are data controllers over the data provided them by subscribers or customers must take reasonable steps to protect customer information against 'improper or accidental disclosure' and must ensure that such information is securely stored. It also provides that customer information must 'not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations.'

---

[17]F.H. Cate, P. Cullen, V.M. Schonberger *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* 2014<Retrieved from: https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf>.

[18]A.B. Makulilo, *African Data Protection Laws* [2016] Springer International Publishing AG; B.U. Udoma, B. Osagie B. (2007). *Data Privacy Protection in Nigeria* [2007]<https://www.uubo.org/media/1337/data-privacy-protection-in-nigeria.pdf> Accessed 23/1/2022.

[19] No. 26 of 2003.

[20]Nigerian Communications Commission, *General Consumer Code of Practice* 2018<https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/drafts-regulations/780-consumer-code-of-practice-regulations-2018/file>Accessed 07/01/2022.

From the foregoing, there is no principal data privacy or protection law or data protection authority in Nigeria; NITDA is the data protection authority under the NDPR 2019 that it issued, however, as a regulation, it does not have the force of law and this limits it in terms of addressing conflicts that may arise in matters of data breaches. Similarly, NCC, the National Identity Management Commission (NIMC), the Central Bank of Nigeria (CBN), and the Federal Ministry of Health are data protection authorities of the telecommunication data, National Identification Number (NIN), financial services data and health records respectively. The danger here is that gaps that may arise across the data and privacy protection value chain as some key aspect of the data and privacy protection may not be addressed since certain sectors or industries do not have a law or legislation addressing their issues in this regard. Additionally, there will be duplication of efforts with its attendant cost of resources.

Table1 is a list of data protection laws and regulations, information they seek to protect and the sections that address such protection.

Table 1: Data and Privacy Protection Laws in Nigeria

Law	Information Protected	Applicable Section
Constitution of the FRN 1999	General	The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected- section 37
Child Rights Act 2003	Child data	Every child is entitled to his privacy, family life, home, correspondence, telephone S.8(1) conversation and telegraphic communications Accordingly no information that may lead to the identification of a child offender shall be published-section 205(2)
FOI Act 2011	Personal Information with public institutions.	A public institution must deny an application for information that contains personal information and information exempted under this subsection includes: (a) files and personal information maintained with respect to clients, patients, residents, students, or other individuals receiving social, medical, educational, vocation, financial, supervisory or custodial care or services directly or indirectly from public institutions; (b) personnel files and personal information maintained with respect to employees, appointees or elected officials of any public institution or applicants for such positions; (c) files and personal information maintained with respect to any applicant, registrant or licensee by any government or public institution cooperating with or engaged in professional or occupational registration, licensure or discipline; (d) information required of any tax payer in connection with the assessment or collection of any tax unless disclosure is otherwise requested by the statute; and information revealing the identity of persons who file complaints with or provide information to administrative, investigative, law enforcement or penal agencies on the commission of any crime-section 14
Cybercrimes Act, 2015	General	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-section 38(5)
Credit Reporting Act, 2017	Credit Information	Unless this Act provides otherwise, data subjects shall have the right to the privacy, confidentiality and protection of their credit information-section 9
National Health Act, 2014	Patients Health Information.	All information concerning a user, including information relating to his/her health status, treatment or stay in the health establishment is confidential

FIRS Act 2007	Tax payers	A person in possession of or control, of any document; information, return of assessment list or copy of such list relating to the income or profits or losses of any person, who at any time communicates or attempts to communicate such information or anything contained in such document, return, list or copy to any person-section 50(2)
Consumer Code of Practice Regulation 2007	Telecommunications Subscriber data	Collection and maintenance of information must adhere to the fair information practices principles as stated in section 35(1a-h) and (2a-d). Licensees must adopt and implement internal data and privacy policies and ensure that the third parties with whom they may exchange consumer information have adopted same policies-section 36
NIMC Act 2007	National identity information of citizens	No person or body corporate shall have access to the data or information contained in the database with respect to registered individual entry except with the authorization of the commission which will be based on the consent of the individual or on account of national security, prevention or detection of crime-section 26(1-3).

9. Sufficiency of Current Data and Privacy Protection Laws

Although there are variations in the data protection laws across countries and regions, there are key elements in the subject matter that are shared across the globe; most especially that data flow across borders is common place in the digital economy. When these key elements are lacking, the law(s) cannot sufficiently address data protection issues across national and transnational concerns. The data protection laws in Table 1 have addressed a couple of data and privacy concerns in Nigeria, however, there are many other key areas left unaddressed and can be of monumental consequences to data subjects with national cascaded effects. The identified gaps are pointed out below:

i. Major personal data collection organisations like the National Population Commission (NPC), the Nigerian Immigration Service (NIS), etc. have no clause in their laws that address data protection. Data collection organisations at the state and local government levels may have no legislations covering the protection of collected data. Similarly, there are several private entities within the SMEs realm that collect, process and transmit data that are not adequately covered in the current legal regimes.

ii. There are concerns that business entities operating in countries other than theirs' may transfer data abroad, this data may end in the hands of third party entities unknown to the data subjects and raise privacy and protection issues[21] however, none of the laws stated in Table1 addressed this concern.

iii. Except for the recently enacted Credit Reporting Act, 2017, most of the laws do not make specific references to data collected, processed and transmitted through ICT or specific types of electronic communications, such as e-mail, cell phones, private communications carriers, CCTV cameras and computer transmissions considering their unique peculiarities of trans-border flow and ease and anonymity of remote accessibility and exposure to special kinds of violations. This have the potential of leaving this aspect unprotected even in the presence of these laws.

iv. There is a strong nexus between technological advancement in ICT and data protection such that new technologies may throw up new challenges in the data protection arena. According to Davies,[22] technologies like cloud computing, Internet of Things (IoT), Big Data Analytics and the ever-expanding sphere of social media have thrown up new and intriguing challenges in data and privacy protection, there is no mention of them in the data and privacy protection laws in Nigeria.

v. The ECOWAS data protection Act addressed concerns on data gathered, processed, stored and transmitted for the purposes of journalism, research and artistic enterprises, however, none of the surveyed local laws in Table1 addressed this aspect of data management.

[21] UNCTAD, 2016.

[22] Ron Davies, Briefing The Internet of Things Opportunities and challenges. *European Parliamentary Research Service* [2015]<http://www.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf>Accessed 07/1/2022.

vi. Establishment of institutional framework is advocated in global, regional and sub-regional entities concerned with data and privacy protection. The laws in Table1 did not address the concern of establishing a Data Protection Authority capable of administering data protection concerns on the data collection, processing, storage and transmission on the data processing value chain as well as delineating clearly the roles, obligations and the rights of the entities involved in the data processing.

vii. The EU-GDPR and other data protection laws, principles and guidelines all advocate the rights to rectification or destruction also referred to as right to erasure or right to be forgotten, the surveyed laws in Nigeria did not address any of these important rights of data subjects.

viii. The education sector through schools and tertiary institutions is a huge repository of personal data of natural persons during their studentships and pupilships, these data is perpetually held by the institutions. However, there is no law that specifically addressed the data and privacy of records held and transmitted in this area.

ix. Issues of data portability across entities and even abroad are not adequately addressed; data subjects are as well unaware of their various responsibilities and rights in the entire scheme as none of the surveyed laws attended to these concerns.

10. Analyses of Overlaps

A few points of overlaps exist in the surveyed laws in Table1. For instance, the Cybercrime Prohibition Act 2015 did not specifically addressed any concern on data and privacy protection, except that it alludes to that which is already covered by section 37 of the 1999 Constitution of the FRN concerning the privacy of citizens. Similarly, section 14 (1d) of the FOI Act 2011contains a repetition of the laws already stated in S.50 of the FIRS Act 2007 addressing tax payers data.

11. Future Research Directions

One of the major challenges of data protection, privacy and confidentiality in the internet era is the borderless nature of the Internet technology that creates jurisdictional problems in addressing trans-border breaches. Breaches on the technology space are essentially global as criminally minded individuals or organisations can perpetrate crimes on data from any part of the world. Consequently, further research should be directed at enacting laws that will break jurisdictional barriers at regional and global levels. Further, from a technology perspective, research should be focused on developing privacy aware solutions that will ensure that data subjects are alerted on the processing and transmission of their data wherever it is held and processed.

12. Conclusion and Recommendations

Personal data is the fuel that powers international trade and e-commerce in the new business models that are ICT driven. Similarly, e-government operations also rely heavily on personal data of citizens to deliver services across government enterprise. This have brought tremendous gains by removing the barriers of time, location and excessive cost of doing business and accomplishing social interactions across the globe. However, the threats of accessing these data illicitly have the potential to undermine these gains by causing users to lose trust in the system and holding back their data to seek safer alternatives. These challenges are further compounded by lack of clarity on where to seek redress when an individual's personal data is violated. Technological safeguards have failed to provide the needed protection, therefore, the only feasible alternative is to offer a plain playing field through legislations that gives all stakeholders on the data management ecosystem a voice. Many countries even in the developing world have towed the path of enacting and implementing principal legislations in this regard, while some, including Nigeria are still at the draft stage. The Nigerian data protection bill has been in the draft stage for about a decade. The existing fragments of legislations and regulations do not speak to the privacy concerns of the information society and may stand on the way of the growth of international trade, e-commerce and e-government in Nigeria. It is hoped that the authorities will expedite action and treat the matter of making this law and its implementation a national emergency. This will restore trust and boost confidence among stakeholders – locally and internationally.

In order to address the challenges arising from the absence of a principal legislation on data privacy and protection and data protection authority in Nigeria; the following are hereby recommended:

i. There should be a single principal data and privacy protection law that addresses national concerns on the data processing value chain. This should subsequently give birth to a Data and Privacy Protection Authority (DPPA) that will ensure the implementation of the data protection laws. This will be in response to global, regional and sub-regional calls on this subject, so as to harmonise the

Nigerian data and privacy protection laws with those of other nations to tackle the trans-border nature of the data protection concerns.

ii. The new law should address all insufficiencies of the existing laws, especially in ensuring that there is a blanket coverage of all organisations that currently and will in the future deal with personal data to a reasonable extent. Specific attention should be given to data transfers to other jurisdictions as well as address storage of data on the cloud where the servers may be resident in other jurisdictions other than Nigeria.

iii. The existing laws addressing data protection concerns in their various spheres in Nigeria should be further and regularly re-fined to address the ever-changing realities of the information society and electronic data collection, processing, storage and transmission.

iv. To arrest the dart of manpower shortage in the data and privacy protection space, which may be a stumbling block to speedy implementation of the data protection law, there should be national efforts across all levels of governance in public and private sectors to train legal practitioners, law enforcement and ICT personnel in the art of data and privacy protection. This is particularly important as it will drive the implementation process should the data and privacy legislation be passed. accented into law.

v. Organisations must begin the process of developing and implementing internal policies for data and privacy protection. They must create awareness among their employees on issues of data and privacy protection stating clearly consequences of violating individuals' personal data on businesses, as it erodes trust, bring sanctions and litigation causing revenues to nose-dive. This will be achievable where there is in existence, a central data protection legislation.