Onyeajuwa, Martha Kanene

Conference Paper

Critical Assessment of Institutional and Regulatory Frameworks for Personal Data Protection in Digital Platform ecosystem: a study of Nigeria

22nd Biennial Conference of the International Telecommunications Society (ITS): "Beyond the Boundaries: Challenges for Business, Policy and Society", Seoul, Korea, 24th-27th June, 2018

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Onyeajuwa, Martha Kanene (2018) : Critical Assessment of Institutional and Regulatory Frameworks for Personal Data Protection in Digital Platform ecosystem: a study of Nigeria, 22nd Biennial Conference of the International Telecommunications Society (ITS): "Beyond the Boundaries: Challenges for Business, Policy and Society", Seoul, Korea, 24th-27th June, 2018, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/190424

Critical Assessment of Institutional and Regulatory Frameworks for Personal Data Protection in Digital Platform ecosystem: a study of Nigeria

Martha Kanene Onyeajuwa**,** PhD

ABSTRACT

Platform ecosystem has spawned a rapidly growing data-driven economy across the globe. The emerging platform models have been adjudged to have a positive impact on quality of life by engendering economic growth. However, as technologies become more intelligent and intrusive, there is a progressively higher risk of personal data being misused or compromised. This paper seeks to study the extent to which personal data is protected in Nigeria using document analysis and complementary conversational interviews, whenever the need arises.

This study finds that regulatory frameworks in Nigeria are not sufficiently focused in addressing the issues of personal data protection when compared with principles of best practice in privacy and data protection. In addition, the players (financial entities and telecoms) do not abide by fair information principles; thus, customers and citizens remain uninformed about their rights, the potential harms inherent in the services on offer and in the choices they make. The absence of a robust enforcement institution leaves the emerging platform ecosystem virtually unregulated, which provides the platform players opportunities in exploitative use of consumer data.

This paper argues that lack of personal data legislation in Nigeria constitutes an obstruction to the realisation of section 37 of the 1999 Nigerian Constitution, which provides for citizen privacy and data protection. The paper further argues that the Communications regulatory framework, by limiting personal data offence to mere ST regulation 2011 infringement, plays a critical role in abstrusely commodifying customer data in ways potentially detrimental to customers.

The lack of a clear legislation, despite the guarantee of citizen privacy and data protection by the 1999 Nigerian Constitution, is an indication of policy failure.

Thus, this paper's focus on personal data protection is important, given the growing significance of digital platform ecosystem across the globe including Africa.

Key Words: Personal data protection guidelines, platform economy, Digital Financial Services, International Telecommunication Union, Nigerian Communications Commission, Central Bank of Nigeria,

1. Background

Nigeria, with a youthful population, between 15 – 35 years, which adds up to 37% of total population of about 174 m people, has the largest economy in Africa and 23rd largest in the world. Nigerian mobile telephone, with average growth rate of approximately 10m lines annually, is rated one of the fastest growing in the world. The preferred mode of communication in Nigeria is by mobile phone with 160.5 million subscribers and teledensity of 114.66 (NCC, n.d.-a).

In the last two decades, Nigeria has been formulating as well as putting in place key institutional policies and regulatory frameworks to drive innovations and widespread use of ICTs by both private and public establishments, businesses, local and international communities. The communications sector anchors the key function of provision of ICT infrastructure for seamless interconnections and efficient operations of all sectors of the Nigerian economy. In 2001, the Nigerian Communications Commission (Commission) licenced four digital Mobile Network Operators whose market shares in April 2018 are: – MTN/41%, GLOBACOM/25%, AIRTEL/24% and 9mobile/10%.

In 2013, the Federal Government of Nigeria (FGN) launched the National Broadband Policy Implementation Strategy for effective nationwide broadband deployment, and the Open Access Next Generation Broadband Network model, which allows for inclusive, fair and transparent licencing process as well as offer incentives to existing and potential investors without discrimination. This strategy is generating impressive growth in Internet users. In April 2018, the total number of Internet subscribers stood at 101.2 million (NCC, n.d.-a).

Internet, which enables operations in real time, is the precursor of the digital ecosystem. Thus, in developing countries like Nigeria, broadband penetration extends ICT services accessibility and facilitates internet inclusion for the unserved, underserved, unbanked and underbanked segments of the population enabling them to benefit from Digital Financial Services (DFS) and subsequently participate in the growing digital ecosystem (David-West & Taiwo, 2018; USPF, 2013; ICT, 2012; CBN, 2013). Digital technology continues to shape multiple dimensions of our lives such as behaviour, needs, views, knowledge sharing, choices etc, which influence the market structure as well as contribute to the Nigerian economy landscape, as is witnessed globally (Evans, 2016, David-West & Evans, 2016; Evans & Gawer, 2016; Kenney & Zysman, 2016; Cohen, 2017).

However, despite the rhetoric surrounding these benefits, the platform business models, seem to possess the dual function of empowering the enterprises and disrupting the industries they operate in (Cohen, 2017; De Groen, Kilhoffer, Lenaerts & Salez, 2017; Srnicek, 2016). The enterprises, for instance, take advantage of their powers to control supply of goods in high demand, become dominant players in the ecosystem and undermine competition by under paying workers (De Groen, Kilhoffer, Lenaerts & Salez, 2017; Srnicek, 2016). There have been other concerns such as creating the possibility for enterprises to take advantage of the gaps in the existing rules: exploiting the right(s) of customers by monetising, at little or no risk on their part, customers' data without securing their consent (Slvy, 2018, Srnicek, 2016).

The highlighted issues emanating from the platform ecosystem seem to suggest the need for effective institutional and legal frameworks that would ensure adequate consumer privacy and data protection in Nigeria. While the developed countries already have legislations on consumer privacy and data protection and furthering their effort to improve them, the practice of consumer protection with focus on customer privacy and data protection is still in its infancy in Nigeria and Africa (ITU-T, 2016).

This study, therefore, seeks to answer the question: How effective are institutional and regulatory frameworks for personal data protection in Nigeria?

The rest of this paper is arranged as follows:

The next section gives a brief review of the literature on Privacy and Data Protection framework. Section three discusses the Analytic framework that guides the study while section four discusses the methodology deployed in the study. Section five scrutinises the NCC and the CBN regulatory frameworks which are the directly involved in the collection, disclosure and transfer of consumer data and section 6 concludes the study.

2. Study Conceptual Framework

2.1 Privacy and Data Protection law

The rapid advancement in technological development has radically transformed the way we live our life, interact with others, do our work as well as create value in the economy (Kenney & Zysman, 2016). For instance, organisations applying their business modules are able to collect, store and utilise personal data in scales that are unprecedented while Over the Top Technology (OTT) make it possible for people to provide their personal data publicly and globally.

Technological advancement also brought new challenges for privacy and personal data protection. Technologies are becoming more intelligent and intrusive. With Near Field Communication (NFC) and advanced techniques for inferences and 'linkability' of data there is increasing risk of personal data exploitation and misuse (ISOC & AU, 2018). Hence, the need arises, more than ever before, for jurisdictions to deploy, without further delay, strong and robust privacy and data protection legislation and enforcement frameworks that mitigate abuses on customer data including monetising, disclosing and transferring customer data to unaffiliated third parties without the consumers' consent.

In most African countries, Nigeria inclusive, the right to privacy is protected by the common law. This is visible in the amended 1999 Nigerian Constitution, in section 37, which states: "The privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected". However, this constitutional guarantee on privacy and data protection needs legislative and other supportive frameworks to actualise the objectives. There is no specific law in Nigeria on the processing and use of personal data. Nigeria has no Data Privacy and Protection Act despite the fact that data is now viewed as gold or perceived as a nation's currency in the evolving digital ecosystem. Furthermore Nigeria lack of a robust data management system nudges numerous government agencies/sector regulators such as: Central

Bank of Nigeria (CBN), National Identity Management Commission, Independent National Electoral Commission, Federal Road Safety Corps, Health care centres etc. to collect similar citizen personal data with little or no respect for their rights. Citizens have no control over what data is collected and how their data deposited in respective silos would be used as well as having no clear channel of redress in event of data misuse (Sesan, 2017).

The lack of privacy and data protection law is pervasive in Africa. 26 countries in Sub-Saharan Africa do not maintain a data protection/privacy system (7 are considering the implementation). Among the 13 countries across the Middle, East and North Africa region, do not maintain a data protection and privacy framework; four are considering the implementation. This contrasts with the situation in EU where all countries across Europe maintain a data protection and privacy framework (GSMA, 2018).

2.2 Data Ownership

Customer engagement with digital platform generates huge volume of personal information such as names, telephone numbers, credit card numbers, email addresses while businesses also generate huge customer data through collection of biometric data, travel data, financial data, and fingerprint scans etc. Similarly, data from customers' use of products and services are considered priceless intangible assets for the enterprise (Marshall and Completer Info, 2001 cited in Elvy, 2018). As explained by Technopedia[1] data ownership is fundamentally a data governance process that details an organisation's legal ownership of enterprise-wide data. An organisation or data owner possesses ability to create, edit, modify, share and restrict access to the data. The individual also possesses the ability to assign, share or surrender personal data and all the rights to a third party and/or withdraw same.

The perplexing question remains: who owns the data or who has right over the data that an organisation collects from the customer: the customer or the organisation?

The researcher is urged to respond the customer, and not organisation, owns customer data since the data was collected directly from the customer. The UK ICO (2017:6) suggests it is important that: "individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced".

A consumer's personal information belongs to the consumer. This is self-evident but may need to be asserted in some cases as in section 38 (2) of Subscriber Telephone Regulation 2011, which confirms consumer ownership of data by mandating licensees to provide reasonable and appropriate consumer access to personal data to effect corrections.. However, the views of scholars on this question are divergent. Some scholars, including Westin (1967) argue that personal data be treated as property and Vera Bergelson contends that "individuals have a stronger moral claim to personal information than collectors" (Bergelson, 2003 cited in Elvy, 2018:464) However, several Privacy law scholars contend that customers do not have property interest in their personal information. Similarly, some experts in the United States argue that personal information is valueless hence customer cannot expect compensation (Elvy, 2018)

[1] https//www.techopedia.com

Currently, as strong scholarly debates: for and against consumer data ownership rage on, the emerging personal data economy models have developed the capacity to enable customers sell, organize and monetize their personally generated information. These emerging models permit customer data ownership as well as customer data compensation (Mobile Forum, 2016). Consequently, any abuse of personal data or exploitation through monetisation should constitute an issue of data ownership, in addition to being a personal data protection issue (Deloitte, 2016).

2.3 Privacy and Data Protection Framework

The rapid advancement in technological development has radically transformed the way we live our life, interact with others, do our work as well as create value in the economy (Kenney & Zysman, 2016). For instance, organisations applying their business modules are able to collect, store and utilise personal data in scales that are unprecedented while Over the Top Technology (OTT) make it possible for people to provide their personal data publicly and globally.

Technological advancement also brought new challenges for privacy and personal data protection. Technologies are becoming more intelligent and intrusive. With Near Field Communication (NFC) and advanced techniques for inferences and 'linkability' of data there is increasing risk of personal data exploitation and misuse (ISOC & AU, 2018). Hence, the need arises, more than ever before, for jurisdictions to deploy, without further delay, strong and robust privacy and data protection legislation and enforcement frameworks that mitigate abuses on customer data including monetising, disclosing and transferring customer data to unaffiliated third parties without the consumers' consent.

The degree to which consumer information can be abused, exploited, disclosed or transferred to a third party in connection with a financial transaction or monetization scheme would to a large extent depend on the prevailing regulatory frameworks and the terms and conditions of an enterprise privacy and data protection policy. Hence, data protection and privacy policies together with communications and financial regulatory frameworks play a critical role in preventing the commoditisation of consumer data in ways that are potentially detrimental to consumers (Elvy, 2018)

This perceived detriment to consumer's wellbeing has engendered several national and international frameworks on consumer Privacy and Data protection. The international frameworks include, the Council of Europe's Convention 108, Organisation for Economic Co-operation and Development (OECD), and the Asian-pacific Economic Cooperation (APEC) Privacy Frameworks. These frameworks have established the internationally accepted standards for online privacy and data protection strategies (ISOC & AU, 2018).

The African Union (AU) has always been committed to policy harmonisation across her member states. However, only few AU members (15 out of 54) adopted the 2014 AU Malabo Convention guidelines on Cyber Security and Personal data. The Privacy and Personal Data Protection Guidelines for Africa was jointly developed by the African Union Commission (AUC) and the Internet Society (ISOC) with contributions from regional and global privacy experts, academics and civil society groups (AUC & ISOC, 2018:2). Article 13 of the Malabo convention identifies

six principles on data protection which align with the eight principles of the EU General Data Protection Regulation (GDPR).

These eight principles have been deployed in over 100 countries and are widely accepted as providing: "a solid foundation for online privacy policies and practices" (ISOC & AU, 2018:6). They form the basis of guidelines adopted by the Commonwealth, the United Nations General Assembly as well as being in line with the European Union's General Data Protection Regulation 2016 (ISOC & AU, 2018). The eight principles of lawful processing and use of personal data are:

> 1) Collection limitation, 2) Data quality, 3) Purpose specification, 4) Use limitation 5) Security safeguards, 6) Openness, 7) Individual participation, 8) Accountability

The EU General Data Protection Regulation (GDPR) has been causing some waves around the world since 2016. GDPR rules provide protection to EU citizens irrespective of where the data travels to. It applies to: processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU (ICO, 2017:6). The implication is that, from 25th May 2018, any company, anywhere, whose database includes EU citizens' personally identifiable information is bound by the GDPR rules. The GDPR places specific legal obligation on both processors[2] and controllers[3] such as legal obligation if the processor is responsible for a breach. The GDPR places additional obligations on controllers to ensure their contracts with processors comply with GDPR.

2.3.1. Analytical Framework

The analytical framework that guide the study are adopted from the Personal Data Protection Guidelines for Africa which was jointly developed by the African Union Commission and the Internet Society, in 2018, as a follow up on the Malabo Convention and the commonly Identified Consumer protection themes for digital financial services developed by the ITU Focus Group on Digital Financial Services in 2016.

The framework adopted from the Personal Data Protection Guidelines for Africa mentioned above consists of the following indices of best practice:

- Lawful and fair processing
- Consent and legitimacy
- Purpose, relevance and retention of data
- Accuracy of data over its lifespan
- Transparency of processing
- Confidentiality and security of personal data

The policy framework for analysing Data Protection and Privacy in the Digital Financial Services include the following indices:

- Clear policy on data collection and sharing
- Encryption of data

[2] Processors-are responsible for processing personal data on behalf of a controller
[3] Controllers-determine the purpose and means of processing personal data

- Access restriction to consumer data
- Protection of personal data
- Informed consent
- Minimization of data collection and limitation of retention

The indices listed above are aligned with the EU GDPR and the guidelines of other key international bodies e.g. the OECD. The regulatory provisions of the financial and telecoms sectors, the major players of the platform ecosystem, are examined and compared with the above principles of best practices.

4. Study Methodology

This study is conducted using investigative inquiry of policy and legal documents of the two key sectors involved in the digital platform businesses evolving in Nigeria. In addition, insight was drawn from key publications and research conducted by experts and international bodies such as the International Telecommunication Union (ITU), the OECD and ICO.

A qualitative single-case study method was adopted to study the regulatory frameworks for digital platform with focus on privacy and data protection involving two sectors of the Nigerian economy (Sutherland, 2016; Yin, 2014). The sectors are the Banking sector, with focus on the Digital Financial System (DFS) and the Communications sector with focus on internet industry. The two sectors are chosen on the basis that they have been identified to play major role in the Digital Financial ecosystems globally, and in Nigeria too (ITU-T 2015). The regulators for the sectors are the Central Bank of Nigeria and the Nigeria Communications Commission, respectively.

The case approach allows this contemporary phenomenon of personal data protection to be studied within a "real-life context", the DFS in Nigeria (Yen, 1994:130). In the process of the study, complementary interviews or conversion with a purpose were undertaken with key policy makers and stakeholders within and outside the sectors mainly for clarification purposes, wherever the need arises during document analysis.

5. **Discussion of findings**

The constitution of the Federal Republic of Nigeria, 1999 (Amended), in section 37 established the citizens' right to privacy. It is important to note that 19 years after, Nigeria has no privacy and data protection law to safeguard individual right to privacy as it relates to personal information during transactions with government and businesses. Consequently, in Nigeria, as in other African countries, there are abundant opportunities for leakage and abuse of personal data to the detriment of the individual (Makulilo, 2015 cited in ITU-T FG, 2016). Various public agencies and private businesses collect, retain and process personal data without a subsisting legislation on Privacy and Data Protection.

This is the case with the mandatory SIM registration, Bank Verification Number (BVN), National identity and Voters registration exercises etc., which have placed consumers' personal information and biometrics in the hands of the telecommunications and financial sectors regulators, government agencies, Mobile Network Operators, banks and their agents. At the point of

registration in these exercises, both biometrics and personal data of individuals were captured. In the case of SIM registration, the Mobile Network Operators (MNO) retain the personal information while the biometrics are forwarded to Commission (GSMA, 2016). These official data controllers and data processors collect, retain and share individual personal data with myriads of public and private organisations (for example law enforcement agencies, insurance, health and educational institutions etc.). In these exchanges, personal data are exposed to abuse. For instance, it is reported that in Uganda the government agencies sell personal information to businesses (Makulilo, 2015 cited in ITU-T, 2016). In Nigeria, it was highlighted in the monitoring and enforcement activities report of the Commission, that all four Mobile Network Operators were indicted and penalised with fines, for selling pre-registered SIMs (NCC, 2014). In like manner, Nigerian businesses collect, store and share customer information as they deem fit in the absence of a subsisting privacy and personal data protection legislation.

Nigeria does not have a central database (GSMA 2016; ITU-T, 2016). Consequently, personal data, collected by private entities and those mandatorily collected by government agencies are stored in separate data collectors' silos without coordination. In the absence of any privacy and data protection legislation, this portends grave abuse and harm to citizens (Elvy, 2018; Omotubora, 2015).

In the prevailing scenario, the only resort for regulators and individuals, regarding privacy and personal data protection, are pieces of regulations and guidelines spread over several policy documents of the telecommunications regulator and those of the financial sector regulator. In this section these regulations are examined to ascertain their adequacy with regard to privacy and data protection.

5.1 Digital financial services

A Digital Financial Service (DFS), the foyer of the platform ecosystem, is a new area for regulators in the financial sector in Nigeria (ITU-T, 2016). Its reliance on mobile networks and broadband internet infrastructures and platforms brings it into the region of regulatory overlap thereby, making Mobile Network Operators (MNO) key players in the digital financial ecosystem. In this antechamber of the platform ecosystem, appropriate legal and regulatory framework are crucial for the protection of consumers in DFS. An important aspect of consumer protection in this regard is safeguarding consumer privacy and personal data because consumer trust and confidence in the system are vital to sustained growth of the sector.

As DFS transactions progresses from one player to the other, consumer data, which is hosted by MNO and the banks and shared with agents and other enterprises, is exposed to potential abuse. Each node in the transaction is a potential source of breach which may result in data abuse and misapplication. Data abuse harms the consumer in many ways. It may result in identity theft, unauthorised access, damage the user's credit profile, unsolicited offers, nuisance calls, fraudulent messages and fraud, commoditization of customer's data (Danbatta, 2015)

ITU-T FG (2016) identified four main themes of laws and regulations in DFS which relate to consumer protection. These are

- Provision of information and transparency
- Fraud prevention
- Dispute resolution
- Data privacy and protection.

In the operation of traditional banking in Nigeria, the focus of consumer protection is security of transaction and fraud prevention. Customer's privacy and data protection did not draw much attention and hence scanty provisions was accorded to it. This situation is still reflected in recent regulatory frameworks in digital financial services as is shown in Table 1. Data privacy and protection in DFS "is in very early stages, with few guidelines and regulations in existence" (ITU-T, 2016:6).

There is no comprehensive and clear policy on Customer privacy and data protection. What obtains in practice is that regulations and guidelines on some bank products and services make references to one aspect or the other of customer data protection. In 2014, the CBN, the financial sector regulator, issued the framework on Bank Verification Number. Under this regulation banks are mandated to collect customers' biometric and demographic data in addition to the tradition customer identifiable data, which banks routinely collect at the point of opening a new customer account. The BVM gives a unique number identity to each account holder in Nigeria.

Table 1 Regulatory framework in data protection in Digital Financial Services

	DATA PROTECTION ISSUES	GUIDELINES AND REGULATION
1	Clear policy on data collection and sharing	Nil
2	Informed consent	Nil
3	Limitation of data collection and retention	Nil
4	Encryption of data	Regulatory framework for use of USSD: Section 6.0 Guidelines on MMRS: Sections 10 (1-14) Regulatory framework for BVN operations: Section 1.8
5	Access restriction to consumer data	Regulatory framework for MPS: Section (4.1.9.17) Regulatory framework for BVN operations
6	Protection of personal data	Regulatory framework for use of USSD: Section 6.0 Regulatory framework for MPS: Section (2.3.1.2) Guidelines on IMMRS: Section 15(e)

7	Consumer education	Guidelines on IMMRS: Section 15(d)

Source: adapted from ITU-T FG-DFS, 2016

Although one of the stated objects, in Section 1.2 (iii) of the BVN regulation 2014, is to define access, usage and management of BVN information, the regulation is silent on the modalities for sharing and transacting in personal data. The BVN regulation 2014 permits several entities to have access to BVN information subject to CBN approval and the payment of a fee. The entities include Deposit Money banks, Mobile Money Operators, Payments Service Providers, Law Enforcement Agencies, Credit bureaus and other Financial Institutions and entities (BVN framework, section 1.6). These entities would, in the course of operations share the BVN information with their agents and affiliates thereby exposing customer sensitive data to potential misuse and harm that may arise from such sharing. In this scenario it is highly probable that, having invested, by paying a fee, to access customers BVN information, these entities and their agent will seek to make good returns on their 'investment' by monetising customer data, especially since there is no subsisting law on consumer privacy and data protection.

The BVN regulation in section 1.8, stipulates that a party involved in the BVN operations shall put in place encryption of message, secured soft and hardware and adequate security procedure for its information. The party is also to ensure its employee treat all BVN information as confidential. These are weak provisions, considering that there are no specific provisions stipulating the conditions for sharing or prohibiting the commoditization of BVN information. The gaps noted above in the BVN regulations pervade other regulations in the banking sector.

5.2 Privacy and data Protection in the telecommunication landscape

In the telecommunication sector, there are a handful of regulations guiding Consumer Privacy and Data Protection. The Internet Industry Code of Practice Bill in its chapter on privacy and data protection directs that an Internet Access Services Provider (IASP) shall comply with the provision of Part VI, Schedule 1 of the Consumer Code of Practice Regulation (General Code) 2007. This section of the General Code 2007 sets out the responsibility of a licensee in the protection of individual customer data. Similarly, the draft of the revision of the General Code 2007 – Consumer Code of Practice Regulation 2018, states that its section on Protection of Consumer Information shall supplement and be read in conjunction with the Registration of Telephone Subscribers Regulation 2011, while the enforcement of the provisions of consumer codes will be in accordance with Chapter IV of the Enforcement Regulations 2005 (General Code 2018, sections 45(9); 68(3))

Hence, in the telecommunication sector, there are four policy documents for regulating Privacy and Data Protection: Internet Industry Code of Practice, Consumer Code of Practice Regulations 2007; Registration of Telephone Subscribers Regulations 2011, and the Enforcement Regulations 2005.

5.2.1 General principles.

Internet Industry Code of Practice Bill stipulates that compliance with Part IV, Schedule 1 of the General Consumer Code of Practice Regulations 2007 (General Code) is mandatory. The General Code 2007 grants Licensees permission to collect and maintain information on individual consumer that is reasonably required for its business purposes. However, the collection, processing and maintenance of personal data are subject to the following criteria which match the principles of the Malabo Convention:

- Fair and lawful collection and processing
- Processed for limited and identified purposes
- Relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with consumers' other rights
- Protected against improper or accidental disclosure
  Source: General Code 2007, Section 35 (a-h)

Furthermore, Licensees are required to declare clearly to the consumer what information is being collected, the use of the information and third-party sharing of that information. Consumers shall be informed of the choices available to them regarding the collection, use and disclosure of their data and the access they have to their data. The transfer of consumer information shall be according to the terms and condition agreed with the consumer or as permitted or approved by the Commission or other relevant laws. The subjective and unspecified nature of some of the conditions listed above, would suggest an efficient monitoring and enforcement framework with appropriate incentives without which compliance may not be achieved.

5.2.2 Fair and lawful collection of consumer data

The General Code, section 43, stipulates that consumer data must be collected and processed lawfully and fairly; taking into consideration the sensitivity of the data collected, consumer other rights and in accordance to the principles set out above. It provides that the IASP shall at all times ensure that the terms and conditions for the use of the data are made open. The Internet Industry Code of Practice (section 4.2), although still a draft code, mandates the Internet Access Service Providers (IASP) to take reasonable measures to protect consumer identifiable information from unauthorised use, disclosure or access. The Draft Code, however, did not give any indication of how 'reasonable measure' is established and from what or whose perspective; data subject, Data Controller or Commission? Neither did it state what level of protection is deemed reasonable.

According to the Personal Data Protection Guidelines for Africa (ISOC & AU, 2018), measures are considered appropriate if they correspond to industry-accepted best practice. It recommends a risk based approach where appropriate measures are evaluated in terms of the risk, likelihood and potential impact of a failure to protect personal data. These guidelines are missing in the Internet Industry Code of Practice (Draft Code): hence the adoption of these recommendation is not assured.

5.2.3 Individual consent

Section 35(h) of the General Code directs that consumer information shall not be transferred to any party except as permitted by any terms and conditions agreed with the customer or the Commission or other appropriate laws.

The issue of consent is a dicey one for individual customers due to information asymmetry. The Terms and Conditions is usually a complex document in technical/legal terms and unlikely to be fully understood by the average consumer. In practice, the terms and conditions of MNO are not disclosed to the customer at the point of purchase and at the registration of the SIM cards and therefore, are not visible to the customer. Moreover, merely presenting information to the consumer about the purpose, use and sharing of personal data, does not guarantee informed and specific consent. Often the purpose for collecting personal data is obscure to the customer who may also, not know how or when their personal data will be shared; or the harms that the sharing entails.

The purpose for personal data collection and processing is crucial for consumer privacy. Hence, personal data must be collected for specific, explicit and legitimate purpose to ensure the contextual integrity of personal data. Data collected in one context and later used in another context without the awareness and consent of the individual breaches an individual's privacy. For example, to disclose or sell a customer's transactional data to another enterprise for commercial purposes; for illegal or fraudulent usage (ISOC & AU, 2018). Fairness of processing indicates that the customer has the right to indicate or enforce his/her preferences regarding whether, when or how personal data moves from one context to another. However, this is not the case in practice. For example, in Nigeria, customers are bound by law to give their personal information to data controllers (e.g. to mobile operators during SIM registration and to banks during BVN and KYC exercises). In these exercises, the controllers are also required by law to share customer data with regulators, government and their agents. In these circumstances, the consumer consent is not required and of no avail.

This is a difficult area for individuals because they have little awareness and no control over the use of the data they provide. Therefore, it beholds government and Data Protection Authorities to enforce ethical principles in the design of both the procedures and services that share or process personal data.

5.2.4 Security and Confidentiality of personal data

The General Code, section 37, further stressed the importance of security of personal data. Its object is to ensure the integrity and confidentiality of personal data i.e. that data is protected from improper or accidental disclosure, alteration or destruction. To this end, licensees that collect identifiable individual consumer information are required to adopt and implement a 'Protection of Consumer Information Policy', regarding the proper collection, use and protection of that information. This provision is expanded in the General Code, 2018 (Draft) to include: Licensees shall also ensure that other licensees or persons with whom they share the data have adopted and implemented an equally appropriate and efficient 'Protection of Consumer Information Policy'.

The implication of this provision is that the licensees are held accountable for personal data they collect, the relocation or transformation of the data notwithstanding. They do not shed their responsibility when they transfer personal data to data processors to process on their behalf; rather the data processors acquire the responsibility of the licensees with respect to the protection of data and the privacy of the data subjects (ISOC & AU, 2018). This puts pressure on all stake holders to adopt and implement industry best practice standards for data security as the appropriate measure to ensure optimal protection of personal data by mitigating the risk of advanced cybercrime inference and 'linkability' schemes.

5.2.5 Data Quality

Section 38 of the General Code holds Data Controllers accountable for the accuracy of customer data held by them. It directs Collectors to ensure that identifiable consumer information is accurate, relevant and current for the purposes for which it is to be used and to put in place appropriate mechanisms for identifying and correcting inaccuracies. These include customer ease of access to inspect data and effect corrections. The General Code's provision falls short of the principle of best practice which, recommends that the access request be handled in a legal framework that safeguards the interest of the data subject. In addition, Controllers are to ensure that customer's personal data is protected against incidental or unauthorised alteration and remains technically accessible. This provision upholds the data subject right to notification, access, correction and erasure (ISOC & AU, 2018).

5.2.6 Informing the Data Subject

The General Code in section 43-44 repeatedly emphasized the responsibility of the data collector to adhere to generally accepted fair information principles. Specifically, the data collector is bound to declare clearly what information is being collected, the intended use of that information, the sharing of that information with third parties and the choice options available to the customer regarding the collection, use and disclosure/sharing of the collected information (General Code section 44 (1-7)). Furthermore, the licensee/data collector's policy is to be made available to the data subject in a readily accessible form and easy to read manner (and I would add) easy to understand plain language. The question, however, remains how much of the information in the General Code and the protection of consumer information policy would the average data subject understand?

Too little or too much information is detrimental to the consumer. This is compounded by the technical and rapidly changing nature of ICT and platform ecosystem. This result is that individuals are not sufficiently informed about their rights, the consequences of their choices when they give their consent. The Commission's Head of Legal Services confirmed that "consumers across the country get ripped off or get into trouble with their services providers because they are not sufficiently informed" (Ogbodo D, 2014). This lack of information leads consumer into trouble, for example, when they accept free service or engage in social media and sign into commercial platforms that collect and monetise their data, (ISOC & AU, 2018).

Individuals have the right to be informed and the responsibility to be sufficiently/appropriately informed to enable them tread cautiously and safely across the internet ecosystem. They also have

the legitimate expectation to be protected as they carry out their normal business online or offline. Asymmetry of information and low individual capacity are great challenges to individuals both in offline and online activities because "the dearth of information that facilitates informed choice leads to consumer detriment" (Onyeajuwa, 2017:648). It presents predaceous business as attractive models; prevent individuals and the country from reaping the dividends of digital ecosystem. More importantly, it undermine citizens' confidence and trust in e-commerce, e-government and other online services.

5.2.6 The role and challenges of regulators and data protection authorities

Asymmetry of information and lack of capacities also constitute significant challenges to regulators, data controllers and other stakeholders. The main challenge to regulators and data controllers is the development of institutional capacity to implement an effective enforcement mechanism that enforces compliance with set rules. Without an effective enforcement institution regulations are of no import (Onyeajuwa, 2017).

The weak institutions and ineffective enforcement processes leave Digital platform ecosystem more or less unregulated. In practice, this laxity in enforcement of rules, provides platform players opportunities to exploitative use of consumer data; to trade customer information through disclosure and transfer to unaffiliated third parties without the customer consent.

In this regard, the development of certification schemes that awards Trustmark as a measure of compliance can encourage providers to compete on the basis/level of performance accordingly to set rules. This type of certification, as recommended by the Malabo Convention, will serve as a help and guide to individual consumers in the decision they make online (ISOC & AU, 2018). It will also engender individuals' trust in e-commerce.

6. Conclusion and suggestions

This paper set out to review the regulatory frameworks in digital ecosystem in Nigeria against the AU Malabo Convention principles of data protection to ascertain the state of privacy and data protection in the emerging digital platforms in Nigeria. The telecommunications regulatory frameworks as provided in the Internet Industry Consumer Code of Practice 2017 (draft code), General Code 2007, and Registration of SIM Card Regulation 2011, are closely aligned with the principles adopted at the Malabo Convention. However, there is no documented evidence that any enforcement sanction has been carried out for any breach of consumer information and privacy. The regulator appears to lack the capacity to enforce the set rules. In addition, the regulator and the Mobile Network Operators do not adhere to fair information principles as a result Data Subjects remain uninformed about their rights and the consequences of their choices.

The regulatory framework in Digital Financial Services is not effective in addressing the issues of data protection in the emerging data-driven economy. It failed to establish a clear policy on how data is to be used and shared. It did not also effectively address the issue of consumer consent and was silent on consumer education. These gaps in the regulatory framework portend harm, undermines the protection of customer data in the emerging data-driven ecosystem.

The absence of privacy and data protection legislation and an independent well-resourced regulatory body, leaves the emerging digital platform ecosystem virtually unregulated with dire consequences for consumer privacy and data protection. This paper suggests that Nigeria, without further delay, adopts the African Union Personal Data Guidelines enacted to implement the Malabo Convention, establish a complementary robust legislation and an independent, well-resourced data regulator as well as deploy adequate incentives including stiff sanctions and effective enforcement mechanisms to prevent exploitation of personal data. A Data Protection Act will bring the various privacy and data protection regulations into a comprehensive document that will be of benefit to an independent and well-resourced Data Protection Regulator, Data Controllers, Data processors and individuals (data subjects) in the varied and growing digital ecosystem.

It is the joint responsibility of all stakeholders to inform and educate consumers on the benefits and potential harms of the platform ecosystem. Therefore, legislative and regulatory provisions should be complemented with well-structured consumer education and awareness programs targeted at different consumer cohorts.

.

Bibliography

Adejumoh, J. (2017, September 28). *Independence*. Retrieved from independence.ng: https://independent.ng/broadband-penetration-hit-30-2018-ncc/

Adepetun, A. (2017, 11 08). *The Guardian*. Retrieved from guardian.ng: https://guardian.ng/technology/53-of-nigerians-lack-internet-access/

Adepetun, A. (2018, March 7). *The Guardian*. Retrieved from guardian.ng: https://guardian.ng/technology/ministry-assures-nigerians-of-30-broadband-penetration-by-year-end/

Amaefula, E. (2018, February 20). *Punch, Buisness and Economy.* Retrieved from Punching.com: http://punchng.com/nitda-to-issue-new-guideline-on-data-protection-soon/

ANEC, BEUC, CI, & ICRT. (2017). *Securing Consumer Trust in the Internet of things: Principles and Recommendations.* ANEC; BEUC; CI; ICRT;.

CBN. (2012). *Guidelines on International Mobile Money Remittance Service.* Lagos: FGN Press.

CBN. (2012). *RegulatoryFramework for Mobile Money.* Lagos: Federal Govt Press.

CBN. (2018). *Regulation for Bill Payment in Nigeria.* Lagos: FGN Press.

Dandatta, U. G. (2015, October 22). *Nigeria Communications Commission.* Retrieved from ncc.gov.ng: https://www.ncc.gov.ng/documents/721-regulators-perspective-on-personal-data-and-privacy-of-users/file

Davies, J., & Szyszczak, E. (2010). Effective protection of consumer rights? *Thomson Reuters (lagal) Limited and Contributors*, 695 - 706.

Deliotte & GSMA. (2012). *Sub-Sahara Africa Mobile Observatory.* London: GSMA.

Deloitte. (2014). *The Deloitte Consumer Review Africa: A 21st Century View.* London: Deliotte.

ECOWAS. (2008, January 16). *ECOWAS: The ECOWAS Conflict Prevention Framework.* Retrieved from womencount4peace.org: http://www.womencount4peace.org/en/legal_documents/frameworks/ecowas_conflict_prevention_framework_ecpf

ECOWAS. (2010). *Supplimentary Act A/A/SA.1/01/10 on Personal Data Protection.* Ouagadougou: ECOWAS.

Elvy, S. (2018, February 28). Commodifying Consumer Data in the Era of Internet of things. *Boston College Law Review, 59*(2/2).

GSMA. (2013). *Sub-Sahara Africa Mobile Economy.* London: GSMA.

GSMA. (2018). *The Mobile Economy.* London: GSMA.

Hantke-Domas, M. (2003). The Public Interest theory of regulation: Non-existance or Misinterpretation. *European Journal of Law and Economics, 15*, 165-194.

ICT.Policy. (2012). *National ICT Policy.* Abuja: Ministry of Communication Technology.

ISOC, & AU. (2018, May 8). *Personal Data Protection Guidelines for Africa: A jiont initiative of the Internet Society and the Commission of the African Union.* Retrieved from internetsociety.org: https://cdn.prod.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

ITU-BDT. (2004). *African Telecommunication Indicators.* Geneva: ITU.

ITU-TFG. (2016). *Commonly identified Consumer Protection themes for Digital Financial Services.* Geneva: ITU.

Mauree, V. (2016). Regulatory Issues for Consumer Protection in Digital Financial Services. *United Nations Conference on Trade and Development.* Geneva: UNCTAD.

NCA. (2003). *Nigeria Communications Act* (Vol. 90). Lagos: The Federal Government Press, Lagos, Nigeria.

NCC. (2014). *Nigerian Communications Commission: Annual Reports and Accounts.* Abuja: NCC.

NCC. (n.d.-a). *Nigeria Communication Commission.* Retrieved from ncc,gov.ng: https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview

NCC. (n.d.-a). *Nigerian Communications Commission.* Retrieved from ncc.gov.ng: https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview

NCC. (n.d.-b). *Nigerian Communications Commission: Enforcement.* Retrieved November 9, 2015, from ncc.gov.ng: http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=1259:enforcement-activities&catid=66:cat-web-legal&Itemid=214

NCCCommunicator. (2014, Quarter 1). *Nigerian Communications Commission.* Retrieved December 28, 2015, from ncc.gov.ng: http://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=frontpage&Itemid=28

NCCCOmmunicator. (2015, Quarter 4). *Nigerian Communications commission.* Retrieved December 21, 2015, from ncc.gov.ng: http://www.ncc.gov.ng/thecommunicator/index.php?option=com_phocagallery&view=category&id=20:2015-quarter-4-gallery

Ndiomewese, I. (2017, March 6). *Techpoint*. Retrieved from techpoint.ng: https://techpoint.ng/2017/03/06/list-tech-hubs-across-nigeria/

NigerianCommunicator. (2015, Quarter 4). *Telecoms Consumers' Bill of Rights,*. Retrieved from http://www.ncc.gov.ng/thecommunicator/index.php?option=com_phocagallery&view=category&id=20:2015-quarter-4-gallery

OECD. (2013). *"Empowering and Protecting Consumersin the internet economy" Digital Economy Papers No 216.* http//dx.doi.org/10.1787/5k4c6tbcvvq2-en: OECD Publishing.

Ogodo, D. (2014, August 18). *This Day.* Retrieved November 9, 2015, from thisdaylive.com: http://www.thisdaylive.com/articles/ncc-why-most-telecom-subscribers-get-ripped-off/186657/

Olowolagba, F. (2018, 03 06). *Daily Post Nigeria*. Retrieved from dailypost.ng: http://dailypost.ng/2018/03/06/nigerian-govt-build-technology-hubs-universities

Onwegbuchi, C. (2018, 01 12). *The Guardian*. Retrieved from guardian.ng: https://guardian.ng/technology/operators-doubt-30%-broadband-penetration-target-for-this-year/

Srnicek, N. (2016). *Platform Capitalism.* Cambridge, UK: Polity.

Sutherland, E. (2016). The case study in telecommunications policy research. *Info* , 16-30.

Take, I. (2012). Regulating the Internet Infrastructure: A comparative Appraisal of the Legitimacy of ICANN, ITU and the WSIS. *Regulation and Governance, 6*(4), 499 - 523.

Van den Bulck, H. (2012). Towards a Media Policy Process Analysis Model and Its Methodological Implicaions. In N. Just, & M. Pupis, *Trends in communication Policy Research: New Theories, Methods and Subjects* (pp. 217-231). Bristol, Uk and Chicago: Intellect.

Williamson, O. E. (1985). *The Economic Institutions of Capitalism.* New York: Free Press.

Yin, R. K. (1994). *Case study research: design and methods.* 2nd edition Thousand Oaks, Calif.; London: Sage.

Yin, R. K. (2014). *Study Research Design and Methods (5th edition).* London: Sage Publication.