ADVOCAAT
LAW PRACTICE

"Proliferation of Data Collection and Storage Agencies in Nigeria – Data Protection and privacy issues"

CONTACT DETAILS:
For further information, please contact the following person at
Advocaat Law Practice:

Rotimi Akapo
LLB (Hons) (LASU) LLM (Cape Town)
rotimi.akapo@advocaat-law.com

T: +234-1- 4531004, 4547932, 2714042
W: www.advocaat-law.com

November 2017

Introduction

A number of agencies, institutions and entities have collected, gathered, stored and or used personal information of Nigerians over the years. The information gathered have been statutorily compelled[1]; obtained in the process of procuring an identity document[2]; volunteered whilst accessing a service[3]; in the exercise of a privilege or a right[4]; or through a combination of all of the above. It is highly probable that the information so obtained by any of the above means have been stored without appropriate technical safeguards and probably used for some other objectives other than that for which it was provided without the knowledge or consent of the data provider, clearly illustrating the inadequate legal, administrative or technical protection against accidental, improper, unauthorized access, disclosure, alteration, use or loss of personal data.

[1] NCC - Registration of Telephone Subscribers, BVN- The compulsion could also either be on the service provider or the beneficiary of the service
[2] NIMC, Immigration, Federal Road Safety Commission
[3] E-commerce transactions
[4] LASRRA, INEC, National Population Commission

The following are some of the agencies and institutions that collect and store personal information in Nigeria:

1. **The National Identity Management Commission (NIMC)**

   The NIMC is to *inter alia,* "create, manage, maintain and operate the National Identity Database".[5] The agency is also responsible for "the harmonisation and integration of existing identification databases in government agencies and integrating them into the National Identity Database".[6] It is also to "ensure the preservation, protection, sanctity and security (including cyber-security) of any information or data collected, obtained, maintained or stored in respect of the National Identity Database"[7]Any person who without authorization or unlawfully accesses any information in the database would be liable on conviction to a term of not less than 10 years imprisonment without the option of a fine.[8]

2. **Nigerian Communications Commission (NCC)**

   Pursuant to section 70 of the Nigerian Communications Act (NCA) the Nigerian Communications Commission (NCC) issued the Registration of Telephone Subscribers Regulations 2011. The objectives of the Regulations[9] are to provide "(*a*) a regulatory framework for the registration of subscribers to Mobile Telephone Services utilising subscription medium in the Federal Republic of Nigeria; and (*b*) for the establishment, control, administration and management of the Central Database."[10]

   All "subscriber information"[11] gathered are to be transmitted to the Central Database[12]. The Regulations provide that the Central Database is the property of the Federal Government of Nigeria, it is domiciled with the NCC and its management, care and control is vested in the NCC.[13]Mobile telephone service providers are however allowed to retain and use subscriber information collected by them on their networks.

3. **Central Bank of Nigeria (CBN) and Financial Institutions - Bank Verification Number (BVN)**

   The BVN project provides each bank customer in Nigeria with a unique identity across the Nigerian banking industry and provides a centralized biometric identification system for the banking industry in Nigeria.[14]

   Subject to the approval of the CBN and the payment of prescribed fees, the following entities may have access to the information in the BVN database - Deposit Money Banks, Other Financial Institutions, Mobile Money Operators, Law Enforcement Agencies, Credit Bureaus, Payment Service Providers and other entities as applicable.[15]

   The Regulatory Framework For Bank Verification Number (the Framework) issued by the CBN merely requires that parties involved in the BVN systems "put in place, secured hardware, software and encryption of messages transmitted through the BVN network", that the data is stored in Nigeria and not routed across borders without the approval of the CBN and that they ensure adequate security and safety of the information.[16]There are no specific sanctions for non-compliance other than the threat of imposition of penalties for any violation[17]

[5] Section 5 (a) National Identity Management Commission Act 2007

[6] Section 5 (a)

[7] Section 5 (g)

[8] Section 28 (2). NIMC claims that as at Sept 6 2017 it had registered over 21.3m Nigerians.

[9] Regulation 2

[10]"*Central Database*" in the Regulations means subscriber information database, containing
the biometric and other registration information of all Subscribers. Regulation 1(2)

[11]Regulation 1(2) "subscriber information refers to the Biometrics and other Personal Information of a Subscriber recorded and stored by licensees or the Independent Registration Agents"

[12] Regulation 6

[13] Regulation 5

[14] There is no law on BVN it is merely a CBN policy or directive. According to NIBSS as at October 22nd 2017, 30.6 million bank customers have been enrolled on the BVN database.

[15]Regulatory Framework For Bank Verification Number (BVN) Operations And Watch-List For The Nigerian Banking Industry – Issued by the Central Bank of Nigeria on 17th October 2017 https://www.cbn.gov.ng/Out/2017/BPSD/Circular on the Regulatory Framework for BVN Watchlist for Nigerian Financial System.pdf

[16] Clause 1.8 of the Framework

[17] Clause 2.3.1 (ii)

4. The Nigerian Immigration Service (NIS)

The Nigerian Immigration Service, amongst other responsibilities, issues travel documents including Nigerian passports to bona fide Nigerians[18]. Applications for Nigeria passports are now made online with the provision of the required information/documents. The NIS has issued a Privacy Policy which can be found on its website[19]. The Privacy policy explains the manner in which the NIS manages the personal information of persons that apply for its services and it is required to be read with the terms of use on the portal. Commitments are made in the policy on protection of personal information provided to the NIS, but no guarantees are provided.

5. Independent National Electoral Commission (INEC)

INEC is statutorily empowered to "compile, maintain and update on a continuous basis a National Register of Voters which has the names of any person entitled to vote anywhere in Nigeria.[20] The information in the register shall be as prescribed in a form by the Commission.

The Voters' Register for each Local Government area is in the custody of the Electoral officer under the general supervision of the Resident Electoral Commissioner.[21]

6. Federal Road Safety Corps (FRSC)

The FRSC designs and issues Driver's Licences in all states of the Federal Republic of Nigeria. Applications for a Nigerian Driver's licence to the FRSC is now online and after the online submission applicants are required to make themselves available for "data capture" where the biometrics of applicants are taken and stored.

In addition to the above, other agencies such as the Lagos State Residents Registration Agency (LASRRA), Motor Vehicle Administration Agency, Nigeria Population Commission, Federal Inland Revenue Service and others have at various times collected, processed and stored personal information of Nigerians.

In most instances and as can be gleaned from above, the laws establishing these agencies, and or institutions that gather, use and store personal information, do not make provisions for data protection privacy of the information provider or where there is any provision for such, they are grossly inadequate to guarantee against unlawful and unauthorized access and or the misuse of such data.

This issue is further exacerbated with the advent of e-commerce transactions where personal information is exchanged on a daily basis. This information are stored, analysed or mined by vendors and or financial institutions to determine purchasing patterns, trends, locations, e.t.c. all without certainty as to the security or safety against the corruption, compromise, unauthorized use and access by third parties or protection for the data subject.

In Nigeria, there is currently no detailed, specific or comprehensive law on data protection and privacy. In some cases there are industry, sector or agency specific attempts to address data protection with the laws/regulations compelling the provision of the personal information also offering some sort of protection for the data collected. However, these provisions are often insufficient and inadequate in protecting against the potential losses or damage that may be inflicted on the providers of such information in cases of compromise, unauthorized access, misuse, loss or disclosure.

Below are some of the existing Data Protection and Privacy Laws, Regulations and Guidelines currently in force in Nigeria.

Section 37 of the 1999 Nigeria Constitution (as amended) – Guarantees and protects the privacy of telephone conversations. The provision appears to protect only Nigerian citizens and has been described as "probably one of the most under-researched, under-litigated and under-developed rights in the Nigerian Constitution."[22]

[18] Section 2 of the Immigration Act 2015
[19] https://portal.immigration.gov.ng/pages/privacy
[20] Section 9(1) Electoral Act 2010
[21] Section 17 Electoral Act

[22] Data protection in an emerging digital economy; the case of Nigerian Communications Commission: Regulation without predictability? Aaron Olaniyi Salau PhD Candidate, Department of Public Law, Faculty of Law, University of Cape Town, South Africa

The Child's Right Act No 26 of 2003–pursuant to the Act "every child is entitled to his privacy, family life, home, correspondence, telephone conversation and telegraphic communications[23]", subject to the exercise of reasonable supervision and control by parents or legal guardians.

The Freedom of Information Act No 4 of 2011[24]– The law is to make public records and information more freely available and accessible to the extent consistent with public interest and the protection of personal privacy and protect the public officers who disclose such public records and information. A public institution is required to deny any request for information that contains personal information[25]. The Act however only covers personal information[26] in the custody or possession of public officials, agencies or institutions.[27]

Cybercrime (Prohibition, Prevention etc) Act 2015 – The law was enacted, amongst other things, for the promotion of cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights[28]. Under the Act, service providers are required to preserve and retain traffic data and subscriber information for a period of two (2) years[29] and release same to law enforcement agencies in accordance with the provisions of the Act[30]. In providing the information to law enforcement agencies however, the service provider is to have due regards to the privacy rights of the individual and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement[31].The Act also provides for fines and terms of imprisonment for intercepting electronic messages[32], unlawful interception[33], computer fraud/forgery[34], unauthorised modification of data and systems interference.[35]

The General Consumer Code of Practice issued by the NCC as a schedule to the Consumer Code of Practice Regulations 2007 - The Code is to guide the production of specific individual codes for services to be provided by telecommunications service providers and serves as a set of minimum requirements for such individual codes. In relation to the protection of the personal information of subscribers, the Code recognizes and restates the internationally accepted general principles on data protection and privacy.[36] The Code further provides detailed complaint submission and handling process for the contravention of any of the provisions of the Code.

The Draft Guidelines on Data Protection 2013 issued by NITDA-The Guidelines apply to data controllers in the public and private sectors and covers the processing of personal data.[37]It is mandatory and applicable to all Federal, state, local government agencies and institutions and private sector organizations that own, use or deploy information systems within Nigeria[38].

The Guidelines cover all organizations that process the personal data of Nigerian citizens within and outside Nigeria and prescribe minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls for such information.

The Guidelines further provides that additional data protection and security guidelines may be developed and used at an organization's discretion in accordance with the Guidelines. The standard internationally accepted data protection principles are incorporated in the Guidelines.[39]

[23] Section 8 (1)
[24] It is ironic that the Act which primarily concerns itself with access to information of a public nature should be considered as one of the legislation that might protect personal information
[25] Section 14 (1)
[26]Personal information" means "any official information held about an identifiable person, but does not include information that bears on the public duties of public employees and official" Section 31
[27] Section 1 (1)The Act further prohibits the disclosure of any information that is subject to (a) legal practitioner-client privilege (b) health workers- client privilege; (c) journalism confidently privilege; (d) any other professional privileges confidently by an Act
[28] Section 1 (C)
[29] Section 38
[30] Section 38(3)
[31] Section 38(5)
[32] Section 9
[33] Section 12
[34] Sections 13 and 14
[35] Section 16 (1)
[36]Paragraph 35 (1)
[37] Personal data is defined as "any information relating to an identified or identifiable natural person ("data subject"); information relating to an individual, whether it relates to his or her private, professional or public life
[38] It however does not cover the processing of personal data concerning public security, defense, national security and the activities of the nation in areas of criminal law.
[39] Section 3

The Registration of Telephone Subscribers Regulation (RTS) 2011 issued by NCC– In compliance with the Regulations, providers of mobile telephone services are required to collect, store and transmit "subscriber information"[40] to the Central Database[41]. In line with the provisions of the Regulations, the Central Database is the property of the Federal Government of Nigeria[42], is domiciled with the NCC who is responsible for the processing of its information and storage.[43] The management, care and control of the Central Database is vested in the NCC.[44]

Mobile telephone service providers are however allowed to retain and use subscriber information collected by them on their networks in accordance with the provisions of the General Consumer Code of Practice for Telecommunications Services and any other instrument issued by the NCC.[45]

In an attempt to provide some assurances on the integrity of the Central Database, the Regulations provide that the administration of the Central Database shall be in accordance with the latest standards issued from time to time by the International Organization for Standardization in relation to security and management of electronics and personal data.[46] The Regulation further provides that the subscriber information shall not be transferred outside Nigeria without the prior written consent of the NCC.[47]

International Standards and Best Practice for Data Protection and Privacy

Internationally, , eight (8) core data protection and privacy principles have evolved over the years in respect of the processing of personal information and several countries have adopted these principles in their laws in one form or the other. For our purposes we shall adopt the principles as provided in Schedule 1 to the Data Protection Act 1998 of the United Kingdom.

The principles as provided in the Schedule are:-

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[48]

In Nigeria these internationally accepted principles and best practice for data protection have been incorporated into the NITDA Guidelines.

The NITDA Guidelines provides that -

1. Personal data must be processed fairly and lawfully

[40]Regulation 1(2) "*subscriber information*" refers to the Biometrics and other Personal Information of a Subscriber recorded and stored by licensees or the Independent Registration Agents

[41] Regulation 11[41]"*Central Database*" in the Regulations means subscriber information database, containing
the biometric and other registration information of all Subscribers. Regulation 1(2)

[42] Regulation 5

[43] Regulation 4(2)

[44] Regulation 5 (2)

[45] Regulation 7

[46] Regulation 6 (2) The Regulations allow subscriber information to be released to security agencies on conditions specified.

[47] Regulation 10 (4)

[48]The principles are also embedded in the EU Data Protection Directive 95/46/EC adopted in 1995 which regulates the processing of personal data within the European Union. The General Data Protection Regulation (GDPR), adopted in April 2016, will supersede the Data Protection Directive and is enforceable from 25 May 2018.

2. Personal data shall only be used in accordance with the purposes for which it was collected
3. Personal data must be adequate, relevant and not excessive
4. Personal data must be accurate and where necessary kept up to Date
5. Personal data must be kept for no longer than is necessary
6. Personal data must be processed in accordance with the rights of data subjects
7. Appropriate technical and organizational measures must be established to protect the data
8. Personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection.[49]

There are almost identical provisions in Section 35 (1) of the General Consumer Code of Practice issued by the NCC and referred to above. The main difference being the requirement that transfer of the provided information to a third party has to be as agreed with the information provider or the approval of the NCC or as provided in any law[50]. These provisions are further referenced in the Registration of Telephone Subscriber Regulations 2011 in relation to the right of telecommunications operators to ""retain and use" the collected subscriber information.[51]

Enforcement and Sanctions

The usual tools for compelling compliance in most jurisdictions are notices, fines, penalties and criminal prosecution for breaches and violations. These are the same enforcement tools adopted in Nigeria by the Guidelines, Regulations and Codes discussed above. Persons whose rights have been violated may commence civil suits for redress. They would however have to rely on the standard rules for establishing claims in civil proceedings as there are no statutory rights of recovery for damages or compensatory provisions in Nigeria for data protection and privacy breaches.

[49] Section 3

[50] The Registration of Telephone Subscribers Regulations also requires the NCC's prior written approval before the transfer of subscriber information outside Nigeria.

[51] Regulation 7 of the RTS

Harmonisation

As detailed above, there are several agencies and bodies that have and continue to collect and store confidential, personal information relating to Nigerians and persons resident in Nigeria. It is also abundantly clear that the multiplicity of these data collection agencies is unnecessary, a drain and an inefficient use of already stretched government resources.

The Federal Government of Nigeria recently set up a harmonization programme with a fourteen (14) months target for the harmonization and integration of all databases operated by all government departments and agencies into the National Identity Database under the management of the NIMC.[52]

Conclusion

The need for the enactment of a specific and comprehensive legal framework for the collection, storage, protection and use of personal data in Nigeria has become increasingly important and urgent due to the risks associated with the likely improper or unauthorized access, disclosure, alteration or loss of such collected personal data both to the individual, businesses and national security interests.

It is an undeniable fact that this data gathering initiatives have provided a very important opportunity and powerful tool for private and public organisations to possess critical business or policy transforming information that can support precise decision making by businesses and government. As the volume of e-commerce transactions continues to increase, the magnitude and quality of information in the possession of private entities will also increase. Businesses can mine this information for increased productivity and profit and there is the possibility of unchecked monetization of stored personal information[53]. Without adequate legislation in place the gathered information could be open to abuse or misuse.

Clearly in Nigeria tenuous protection is afforded personal information or personally identifiable data by Guidelines and Regulations but no

[52] As reported in http://itedgenews.ng/2017/09/24/nigerian-government-moves-harmonise-data-ncc-frsccbn/

[53] See https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

legislation. The eight (8) core principles of data protection and privacy that have developed overtime and are internationally accepted standards should form the fundamental pillars for a law on data protection and privacy law in Nigeria. Nigeria will not be re-inventing the wheels in this respect as there are well articulated, detailed comprehensive and tested laws applicable in several countries like the United Kingdom, USA, Canada, European Union, India and South Africa.

Regulations and Guidelines do not carry the same weight as a duly enacted law. Regulations are secondary legislation which sometimes can be creatively circumvented and Guidelines are just, well guidelines, as they are called, even though they are issued pursuant to the laws establishing the agencies and breaches can be regarded as breaches of the substantive laws .

As these data gathering agencies and institutions cut across several industries, sectors, jurisdictions and regulators in Nigeria as can be seen from our analysis above , there should be an independent statutory body to prescribe, monitor and enforce standards for the gathering, storage and retrieval of information in the custody of the various organizations both public and private[54]. This would provide the required comfort to information providers that that their personal information will be protected and their privacy legally assured.

[54] Similar to the Information Commissioner's Office(ICO) in the United Kingdom and the Information Regulator in South Africa.