Journal of International Technology and Information Management

Volume 26 | Issue 4 Article 4

12-1-2017

Data protection in Nigeria: Addressing the multifarious challenges of a deficient legal system

Roland Akindele
Adeleke University, Ede, rollymack@gmail.com

Data Protection in Nigeria: Addressing the Multifarious Challenges of a Deficient Legal System

Roland Akindele,
Faculty of Law, Adeleke University (AU),
Ede, Osun State.
Telephone: +2347057938580.
Email addresses: roland.akindele@adelekeuniversity.edu.ng;
rollymack@gmail.com.

ABSTRACT

This paper provides an overview of the current state of privacy and data protection policies and regulations in Nigeria. The paper contends that the extant legal regime in Nigeria is patently inadequate to effectively protect individuals against abuse resulting from the processing of their personal data. The view is based on the critical analysis of the current legal regime in Nigeria vis-à-vis the review of some vital data privacy issues. The paper makes some recommendations for the reform of the law.

KEYWORDS: data protection, data privacy, legislation, legal reform, Nigeria

INTRODUCTION

The rate at which Nigerians are being requested to furnish personal data has increased tremendously in recent years. Different government agencies and corporate bodies are involved in the collection of personal data. For instance, Biometric Verification Number (BVN) enrolment is being undertaken by different commercial banks ostensibly to prevent identity theft and secure banking transactions. The challenge is that the law in Nigeria does not adequately provide for data protection and management.

Self-regulation which is an in-house control mechanism adopted by any data-collecting body prevails on privacy issues apart from few sectoral soft codes. Soft codes are regulations that are directory only without any force of law or threat of sanction against any breach. The vital questions that arise are as follows: Is it reasonable to leave this important issue to be subject to self-regulation? How does the legal framework address the challenges of enforcing companies' privacy undertakings about how they collect, use and secure consumers' personal

  ISSN: 1941-6679-On-line Copy

information? Can Nigerians enjoy the same or similar measures of data protection as European citizens currently enjoy? Under the European Data Protection Directive and 2016 General Data Protection Regulation, European citizens are assured of a package of rights, including the right of access to their data, the right to know where the data originated, the right to have inaccurate data rectified, the right of recourse in the event of unlawful processing, and the right to withhold permission to use their data for direct marketing.

Nigeria does not have any *omnibus* data protection law that is comparable to that in operation in other countries like South Africa, Canada and countries in the European Union (EU). In other words, there is no single legislation focusing solely on data privacy regulations in Nigeria at the moment. The closest that Nigeria has to a data protection regulation appears to be the Draft Guidelines on Data Protection published by the National Information Technology Development Agency. Clause 1.2 of the Guidelines provides that the authority for the Regulations is in accordance with the NITDA Act 2007 and that they are issued in pursuance to Sections 6, 17 and 18 of the NITDA Act. It should be noted that the guidelines can at best be described as soft codes as there are no mandatory provisions.

DATA PROTECTION FRAMEWORKS IN NIGERIA AND SOUTH AFRICA

South Africa is arguably the leading country in the continent of Africa in data privacy law. The Nigerian and South African legal regimes in data privacy will be examined for the purpose of drawing differences between the two legal jurisdictions.

THE NIGERIAN SITUATION

Section 37 of the Constitution of the Federal Republic of Nigeria guarantees the protection of the privacy of every citizen. Beyond this constitutional provision, there is no machinery for enforcement. Some vital legal issues have been raised (Kusamotu, 2015) concerning this constitutional provision. First, Nigeria does not have specific privacy laws but the right to privacy is guaranteed in the constitution. Second, this provision is discriminatory against non-citizens. The provision states 'the privacy of citizen. . . ' The question is what happens in the case of the personal data of non-citizens that are being processed or are to undergo processing after being transferred to Nigeria?

More importantly, the second schedule to the Constitution which deals with legislative powers does not provide for information and communication technology

directly. An inference may only be made from some clauses that govern matters like posts, telegraphs and telephones, wireless, broadcasting and television that National Assembly of Nigeria is vested with the exclusive legislative competence on ICT matters. This becomes relevant to our discussion as most data are now being exchanged through ICT media more than ever before.

In Nigeria**,** several attempts have been made to enact a data protection legislation. Many bills have been drafted to address areas within the scope of information and communication technology in Nigeria but none of them has been passed into law yet. Some of the draft bills include the following: the Cyber Security and Data Protection Agency (Establishment, etc) Bill 2008, the Electronic Fraud Prohibition Bill 2008, the Nigerian Computer Security and Protection Agency Bill 2009 and the Computer Misuse Bill 2009.

We shall briefly examine three major legal instruments that are relevant to our discussion, namely the Official Secrets Act, No 29 of 1962, the Freedom of Information Act 2011 and the National Information Technology Development Agency Draft Guidelines on Data Protection.

The Official Secrets Act is a vestige of the colonial administration in Nigeria. It was a legislation designed to make provisions for securing public safety (Jemilohun & Akomolede, 2015). It is noteworthy to point out that out of the nine sections of the Act only two sections bear any iota of relevance to the issue at hand. Section 1 of the Act provides for the protection of official information. However, the section only deals with official information or information belonging to or in the custody of the government. The section also deals with officials of the government compromising information that is classified. Section 9 (1) of the Act interprets the expression 'classified matter' to mean 'any information or thing which, under any system of security classification, from time to time, in use by or by any branch of the government, is not to be disclosed to the public and of which disclosure to the public would be prejudicial to the security of Nigeria'. Therefore, the only category of information that is protected is that which if disclosed would be prejudicial to the security of Nigeria. It is clear that where the information though official or otherwise classified is abused by a person not in the service of the government, such a person is not punishable by the provisions of this law.

The Freedom of Information Act was enacted in 2011. The preamble of the Act describes the Act as "an Act to make public records and information freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy, protect serving public officers from adverse

consequences for disclosing certain official information and establish procedures for the achievement of those purposes and related purposes thereof". Like the Official Secrets Act, the Freedom of Information Act deals with information in the custody of public institutions.

The Act cannot be regarded as a data protection legislation by any standards, as the provisions are not comparable to what obtains in South Africa and the European Community Data Protection Directive mandates member states to consider in legislating for data protection. Relevant provisions of the South African Protection of Personal Information Act (POPIA) No. 4 2013 which governs data protection in South Africa will be highlighted in this paper.

Firstly, the provisions of the Act do not reflect the eight core data protection principles that have evolved globally over the years and which have become the bedrock of data protection legislation around the world.

Every enactment in any part of the world that qualifies for data protection legislation utilizes to a large extent those fundamental principles. Also, the Act does not make provision for any classification of information as private or public; it only talks about 'information that contains personal information'. It is also considered to be a fundamental omission the failure of the Act to make any reference to information in the custody of private organizations or individuals.

The core functionality of most data protection legislation in the present age has to do with preventing abuse of private information by private organizations. In the United Kingdom where there is a freedom of information law like Nigeria a separate data protection legislation is in place. This is due to the perceived differences between a freedom of information law and a data privacy legislation. Significantly, Section 15 (1) of the Freedom of Information Act, 2011 provides that information in public custody 'that contains personal information' shall be denied access. A major gap in the Freedom of Information Act is that where a public institution grants access to 'information containing personal information', no offence is created and therefore there is neither a penalty for such abuse nor a remedy for the party whose personal information is improperly or inappropriately disclosed.

The National Information Technology Development Agency Draft Guidelines on Data Protection was released by the agency in September 2013. The document contains a set of mandatory guidelines for federal, state and local government agencies and institutions as well as private sector organisations which own, use or deploy information systems in Nigeria. The guidelines were issued in pursuance to Sections 6, 17 and 18 of the National Information Technology Development

Agency (NITDA) Act. Any breach of the guidelines is deemed to be a breach of the principal Act. The guidelines further provide that it shall be subject to periodic review by the agency.

The National Information Technology Development Agency was created under the NITDA Act of 2007 as the government agency responsible primarily for the planning, development and promotion of the use of information technology in Nigeria. Section 6 of the Act deals with the functions of the agency. The section stipulates that the agency shall among other things, develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information.

Sections 17 and 18 of the Act provide for offences like failure to comply with the provisions of the Act, failure to make payment as appropriate, liability of officers and the need for the agency to collaborate with the Standards Organisation of Nigeria to enforce the guidelines and standards formulated by the agency.

The claim to data protection by the guidelines is difficult to justify. The provisions of Sections 6, 17 and 18 of the NITDA Act which form the basis for the guidelines are not related to any known data legislation in the world.

The preamble to the Guidelines on Data Protection refers to the mandate of the NITDA as given by the NITDA Act 2007 to develop information technology in Nigeria through regulatory policies, guidelines, standards, and incentives. The preamble states further that part of the mandate is to ensure the safety and protection of the Nigerian citizen's personal identifiable information otherwise known as personal data and a successful implementation of guidelines on data protection.
The Guidelines seek to separate the actual collection of data from its processing. This provision is as irrelevant as unnecessary as it is practically impossible to collect personal data in the electronic world without some sort of processing. These provisions are not radically different from the provisions of Section 2 of the United Kingdom Data Protection Act of 1998.

The guidelines place the responsibility for the protection of the privacy of individuals on data controllers which could be an individual or a legal person such as a corporation, public authority, agency or any other body which alone or jointly with others determine the purposes or means of processing personal data.

The guidelines expressly prohibit the collection of personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of personal data concerning health or sex life except on some conditions. The conditions are that: the data subject has consented explicitly to the collection and processing; or the collection and processing are necessary for the purposes of carrying out the obligations and specific function of the controller in the field of employment; or collection and processing is necessary to protect the vital interests of the data subject or another where the data subject is incapable of giving consent; or collection and processing is carried out in the course of its legitimate activities with appropriate guarantees by a relevant association or other non-profit-seeking body and that the processing relates only to members of the body; or the collection and processing relates to data which are made public by the data subject or is necessary in legal matters.

According to the stipulations contained in the guidelines, where the data was not obtained from the data subject, the controller must at the time of recording the personal data provide the data subject with information about the identity of the controller, the purposes of the processing, further information such as the categories of data concerned, the recipients of such data and the mechanism for access to and rectification of the data concerning him.

The last segment of the Draft Guidelines attempts to provide a set of principles known as *fair information principles (FIPs)* which are the basic principles of data protection. They are as follows:
Principle 1: Personal data must be processed fairly and lawfully;
Principle 2: Personal data shall only be used in accordance with the purposes for which it was collected;
Principle 3: Personal data must be adequate, relevant and not excessive;
Principle 4: Personal data must be accurate and where necessary kept up to date;
Principle 5: Personal data must be kept for no longer than is necessary;
Principle 6: Personal data must be processed in accordance with the rights of data subjects;
Principle 7: Appropriate technical and organizational measures must be established to protect the data;
Principle 8: Personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection.

These eight principles are universally accepted as the foundation of all data protection legislation. From the European Data Protection Directive to the data protection laws of countries like Canada, South Africa and the UK, the above principles are enshrined firmly.

ISSN: 1941-6679-On-line Copy

It must be noted that a careful examination of the NITDA Draft Guidelines shows clearly that the guidelines are grossly insufficient to meet the demands of a proper data protection legislation.

The document does not create legal rights for data subjects though it attempts to create liabilities for organizations that process data. For instance, the provisions of Article 2.2.7 states that "the data subjects shall have 'the option to' object to the request to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing and not the right to object. Section 2.3.6 under the Guidelines for Data Access states that 'any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions pursuant to these guidelines is entitled to receive compensation from the controller for the damage suffered'. The procedure to be followed in this instance is not discussed and mode of assessing the amount of compensation payable is not known. The mechanism for enforceability is not clearly stated in the regulations. Standard enactments in the field of data protection across the world characteristically establish mechanisms for enforcement due to the inclination of data controllers to process data at great risks to data subjects. This view is supported by the positions in South Africa, United Kingdom and countries in the European Union. The various data protection legislations of the advanced economies and other developing jurisdictions created specific mechanisms or institutional frameworks for data protection. The European Union Data Protection Directive in Article 28 mandates each member state to create an independent supervisory agency to monitor the application of data protection laws and to investigate violations. It is a fundamental omission for any data protection regulation so-called not to provide for specific institutional enforcement mechanisms.

THE POSITION OF LAW IN SOUTH AFRICA

African countries with a comprehensive approach to data privacy include Ghana, Kenya, Cape Verde and South Africa (Neethling, 2005).

In South Africa, however, no clear-cut distinction is made between the rights to privacy and data (privacy) protection unlike in the EU (Lynskey, 2014). Data privacy is an integral part of the right to privacy referred to as information privacy. In Europe, there is currently a growing body of jurisprudence that seeks to remove data privacy totally from the realms of privacy (Hert & Gutwirth, 2009). Nevertheless, it is submitted that South Africa's approach is in line with the plain wording of Article 1 of the EU Directive where the right to privacy is reasonably

tied to data protection. The draft EU Regulation in Article 1 (2), however, adopts a different approach, in that privacy and data protection are totally separated. Due to the substantial influence the EU data privacy regime has on South Africa, it may be argued that the conceptual foundation for data privacy is the same in both jurisdictions.

The ground work (*travaux préparatoires*) for the Protection of Personal Information Act (POPIA) comprises very exhaustive discussions on the contents and interpretation of the Act (Abdulrauf, 2014). The South African Law Reform Commission's Privacy and data protection report of 2009 is publicly available.
It is noteworthy to point out that the South African data privacy law has been significantly inspired by the EU regime. The Protection of Personal Information Act (POPIA) is a progressive document which contains elaborate provisions that tackle present and future data privacy challenges.

In South Africa, data privacy is currently protected through the Constitution, common law, sectoral law and soft laws (regulations and guidelines).

DATA PROTECTION LAW IN NIGERIA AND THE DATA PROTECTION LAW IN THE EUROPEAN UNION

There is no doubt that Europe has been leading the whole world in data privacy regulations. Therefore, the legal regime for data protection in Nigeria will be examined in the light of the position of law in the European Union.

We shall briefly consider an overview of the data protection situation in the United Kingdom.

THE UK POSITION

In 1995, the European Commission adopted the Data Protection Directive which aimed to harmonise data protection legislation throughout the European Union. Member States have adopted the Directive in slightly different ways, so there are still some differences in national data protection law between them. Each member state was required to implement the Directive by 24 October 1998.

The Data Protection Act 1998 is the UK's implementing legislation. It provides the framework for the UK's data protection regime

Among other things the Act:

- sets out the rules and practices which must be followed when processing information about individuals;
- grants rights to those individuals in respect of their information; and
- creates an independent supervisory body to enforce these rules, rights and practices.

RIGHTS OF DATA SUBJECTS

The Act confers a number of rights on individuals in respect of their personal data. For example, individuals:

- may make requests to those who process personal data about them (known as "subject access requests") for information as to what data are stored, what it is used for, the recipients to whom it is or may be disclosed and the source of the personal data;
- possess rights to prevent processing likely to cause substantial damage or substantial distress to them or to another;
- possess the right to object to direct marketing;
- possess the right to veto automated decisions which significantly affect them;
- may take action to get their personal data corrected or erased; and
- are entitled to compensation from data controllers for breaches of the Act.

Many breaches of the Data Protection Act 1998 are criminal offences. Further, the directors or other officers of a company in breach may also be personally liable.

There are also other consequences. The level of awareness of individuals in the UK with respect to their data protection rights has increased over the last few years, and people will more readily complain to the Information Commissioner where an organisation is not complying with data protection legislation.

From our discussion so far, it has been demonstrated that there is no legislative enactment in force that is designed ***specifically*** to govern data protection in Nigeria. Where a person's informational privacy rights have been violated or breached, the only main remedy available to such a person is to bring an action in common law. Acts amounting to a breach of privacy may infringe on some rights under common law. It seems the laws of harassment, private nuisance, defamation and confidence may in some circumstances provide remedies for privacy intrusions in some indirect way (Lehdonvirta, 2004). Usually, data protection regimes seek to protect data privacy through the establishment of rights for the individual and obligations

for the data controller. In this respect there appears to be an overlap between data protection and the common law remedies in torts.

Private nuisance may be seen to have some remedies in data protection. In the Canadian case of *Motherwell v. Motherwell* (1976) and the English case of *Khorasandjian v. Bush* (1993) it was used to provide remedies for unwanted mail and unwanted phone calls respectively. For instance, in the English case of *Hunter v. Canary Wharf Ltd*. (1977) it was held that a person must have an interest in land before he can have the standing to sue. It is obvious that the usefulness of this common law action is limited in this digital age. The other areas are the law of defamation and the law of confidence. The law of defamation can provide individuals with means to restrict the publication of some information regarding them, and a remedy after the fact. The drawback is that truth is a complete defence to defamation. However, in the law of data protection, the authenticity of information about a person is not the issue. The issue is that a person wants to keep his or her personal information private.

The law of confidence remains the main way by which misuse of confidential information may be redressed under these circumstances. In 2003 in the English case of *Douglas & Others v. Hello! Ltd. and Others (No 3)* the claimant was awarded damages under both breach of confidence as well as the United Kingdom Data Protection Act 1998. Notwithstanding its merits in privacy protection, the law of confidence is not a substitute for a data protection regime that embraces the complete life-cycle of a piece of personal data, from collection through use to any disclosure.

No legislation in Nigeria appears to have embraced the data protection principles enshrined in the European Convention for the Protection of Individuals with regard to Automatic Processing of Data, European Treaty Series No. 108, Strasbourg 1981or the Data Protection Directive (Directive 95/46/EC of 1995). The legal implication of this is that unlike the scenario in South Africa private data of European Union citizens cannot be moved into Nigeria for any purposes except the exceptions in the European Union Directive are complied with. Transfers to Nigeria will have to come under those exceptions where adequate level of protection is not provided. Having laid down a prohibition of data transfers in Article 25, Article 26, headed 'Derogations' goes to lay down a number of situations in which Member States of the European community must permit transfers and a further set of situations in which they may authorise transfers.

Transfers may be permitted when:

(a) The data subject has given his consent unambiguously to the proposed transfer; or
(b) The transfer is necessary for the performance between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) The transfer is necessary in order to protect the vital interests of the data subject; or

(f) The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Article 25 of the Data Protection Directive prohibits the transfer of personally identifiable data to any third country that does not provide 'adequate' protection. Several multinational corporations do business in Nigeria and some of them have European Union citizens as their employees, residing in Nigeria and transacting business in Nigeria. Article 29 Working Party of the European Union expects such companies to make provisions for the protection of private data. Referring to the possibilities of providing adequate protection, the Working Party comments that "the Working Party would find it regrettable that a multinational company or a public authority would plan to make significant transfers of data to a third country without providing an appropriate framework for the transfer, when it has the practical means of providing such protection". The Article 29 Working Party consists of a representative from the data protection authority of each Member State, the European Data Protection Supervisor, and the European Commission in line with the provision of Article 29 of the Data Protection Directive and it was launched in 1996

Apart from the exceptions mentioned above, there are only two other ways by which European citizens' data may be moved into Nigeria. The first one is where companies based in Europe but doing business in Nigeria undertake to comply with the provisions of the European Convention in the handling of data of EU citizens.

This is what is expected of companies or businesses of European origin by the provisions of the Directive. Article 26 (2) provides that: "... a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection – where the controller adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses".

The second way is where Nigeria as a country is granted similar privilege as is granted the United States under the Safe Harbour Principles. The Principles arise from an agreement put in place by the United States with the European Commission whereby US businesses who sign up to a set of privacy principles (similar to the Data Protection Principles under the EU's Directives) may be considered as offering adequate protection. By this, companies doing business in Nigeria whether of European origin or not are expected to ensure the safety of the data of European citizens by providing protection for personal information which is deemed adequate by the authorities in Europe.

The Safe Harbour Principles emerged in the United States because of the level of protection for personal data that Europe demands but which appears to be against the interest of Americans. Since the prohibition of data flows to the United States from Europe will also mean huge business losses with some unpleasant effects, bilateral negotiations were undertaken leading to some measures of data protection without unduly compromising Americans belief in self-regulation and the marketplace (Kobrin, 2004). However, no one is sure if any European country will be willing to offer Nigeria such privileges because unlike the United States, Nigeria does not have the volume of business that may force or compel Europe to negotiate with Nigeria. Furthermore, the United States has a common denominator with Europe in the field of data protection. The United States is a member of the Organization for Economic Cooperation and Development (OECD) and the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal data has as its primary aim – 'to avoid the creation of unjustified data protection obstacles to the development of economic relations and the trans-border flow of data'.

With the current legal regime on data protection in Nigeria, the data of European citizens cannot legally be processed in the country. A resulting loss arising from this is that software contracts which are being outsourced to other nations like India may not be given to any Nigerian company.

ISSN: 1941-6679-On-line Copy

The legal regime in Nigeria on data protection is so deficient that many issues such as loss of data; identity theft**;** e-commerce; e-health and are left unregulated and data subjects are left with little or no protection against abuse of personal data by data controllers and data processors. This can be contrasted with the position in the UK under the Data Protection Act, 1998.

Customers of financial institutions in Nigeria have been facing the risk of identity theft and cyber financial crimes which are the consequences of the absence of adequate data protection legislation. It has been observed that identity thefts are part of the emerging ICT related crimes in Nigeria which need to be addressed urgently by the government (Arowosaiye, 2008).

Turning to e-commerce, trading on the Internet is made through transmission of electronic data from e-traders to e-consumers and *vice versa*. Hence, protection of such data has been a constant source of concern for Nigerian internet users especially consumers. In a recent research (Downing, 2016), it was demonstrated that the European Data Protection Directive seems to have resonated with consumers as appropriate and complete.

Problems of enforcement of the data protection law in Nigeria can be linked directly to the fact that there is neither a comprehensive data protection law in place nor a Data Protection Authority (DPA) that can drive compliance with data protection principles.

CONCLUSION AND RECOMMENDATION

This paper has attempted to present a need for Nigeria to have a basic data protection law that is focused solely on the protection of the private information of individuals especially in this electronic age. Legislations that deal with information like the Official Secrets Act and the Freedom of Information Act were examined and found lacking the essential ingredients of data protection legislation. The article also examined the recently released draft guidelines on data protection from the Nigeria Information Technology Development Agency and contends that the draft guidelines are not sufficient to replace a proper legislation.

A close examination of the history of the emergence of data privacy law reveals that international institutions with their data privacy instruments have been very influential in the emergence and development of the right to data privacy. It is from the European Union (EU) and some countries in Europe that the notion of data privacy as an independent human right began. Therefore, when it comes to issues of data privacy, the EU becomes a reference point.

It is recommended as follows:

i. With respect to the scope of a proposed data protection law in Nigeria, it is suggested a holistic piece of legislation for the private and public sectors is adopted like the South African approach (Abdulrauf, 2016).

ii. In considering what should be contained in the proposed data privacy law, it is suggested that such a law must adopt a rights-based approach. Where a right is infringed upon a remedy must be provided. In other words, a legal wrong should not go undressed by an appropriate legal remedy.

iii. Since Freedom of Information Principles (FIPs) are fundamental in any data privacy law, sufficient space must be devoted to them in a proposed data privacy law in Nigeria. Indeed, the approach of the South African POPIA shows great insight from a rights-based standpoint as the FIPs are not only made an integral part of the Act but are also made rights of data subjects as provided for in section 5 of the Act.

iv. It is pertinent to point out that the fact that a comprehensive legislation on data protection is enacted is not enough for the realisation of the right to data privacy in Nigeria. There is also the need for an effective oversight institution that monitors and enforces the strict compliance of the law. The need for a dedicated and independent data protection agency or authority (DPA) cannot be over emphasized. It is suggested that a DPA should be established in Nigeria.

v. It is suggested that with respect to the scope of the proposed law, what constitutes *personal information* must be broadly defined in a manner as possible similar to that in the South African POPIA.

REFERENCES

LA Abdulrauf. Do we need to bother about protecting our personal data? Reflections on neglecting data protection in Nigeria (2014) 5(2). *Yonsei Law Journal* 78-81.

LA Abdulrauf. The legal protection of data privacy in Nigeria: Lessons from Canada and South Africa, unpublished Ph.D. thesis, University of Pretoria, 2016.

YI Arowosaiye. The new phenomenon of phishing, credit card fraud, identity theft, internet piracy and Nigeria criminal law paper presented at the 3rd Conference on law and technology, Faculty of Law, University Kebangsaan

Malaysia and Faculty of Law, University of Tasmania, Australia, 11 & 12 November, 2008.

C.E Downing. (2016) "Privacy and The Information Age: A Longitudinal View," *Journal of International Technology and Information Management*: Vol. 25: Iss. 2, Article 3. Available at: http://scholarworks.lib.csusb.edu/jitim/vol25/iss2/3.

P De Hert & S Gutwirth Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action in S Gutwirth et al (eds) Reinventing Data Protection? (2009) 8-10.

BO Jemilohun & TI Akomolede. Regulations or legislation for data protection in Nigeria? A call for a clear legislative framework. (2015) *Global Journal of Politics and Law Research* Vol.3, No. 4, pp.1-16.

A Kusamotu, 'Privacy Law and Technology in Nigeria: The Legal Framework will not meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/46' (2007) 16/2 *Information & Communications Technology Law* 149–59 at 154.

Stephen J. Kobrin. Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies* (2004), 30, 111-131 British International Studies Association.

V. Lehdonvirta, (2004). European Union Data Protection Directive: Adequacy of Data Protection in Singapore. *Singapore Journal of legal Studies*, 511-546

O Lynskey. Deconstructing data protection: the Added-value of a right to data protection in the EU Legal order (2014) International and Comparative Law Quarterly 569-597.

J Neethling. The concept of privacy in South Africa (2005) 122(1). *The South African Law Journal* 18-28.

STATUTES

Constitution of the Federal Republic of Nigeria, 1999.
Freedom of Information Act, 2011.
European Union Data Protection Directive

National Information Technology Development Agency (NITDA) Act, No. 23 of 2007.
Official Secrets Act of 1920.
Official Secrets Act, No 29 of 1962.
Protection of Personal Information Act, No. 4, 2013 (South Africa).

CASES

Douglas & Others v. Hello! Ltd. & Others (No. 3) [2003] All E.R. 996.
Hunter v. Canary Wharf Ltd. [1997] 2 All E.R. 426.
Khorasandjian v. Bush [1993] 3 All E.R. 669.
Motherwell v. Motherwell (1976) 73 D.L.R. 62.