Global Journal of Politics and Law Research
Vol.3, No. 4, pp.1-16, August 2015
Published by European Centre for Research Training and Development UK (www.eajournals.org)

REGULATIONS OR LEGISLATION FOR DATA PROTECTION IN NIGERIA? A CALL FOR A CLEAR LEGISLATIVE FRAMEWORK

Dr. Bernard Oluwafemi Jemilohun*
Faculty of Law, Ekiti State University, Ado-Ekiti, Nigeria

Prof. Timothy Ifedayo Akomolede**
Faculty of Law, Ekiti State University, Ado-Ekiti, Nigeria.

ABSTRACT: *Personal information or personally identifiable data is a subject that people have become aware of the need to protect. And the challenge of legislating for data protection in today's world is that which many nations have taken seriously. Nigeria as a developing nation appears not to be left out of this as the NITDA has released a set of guidelines in this regard as a means to offer some protection. This article examines legislations on the Nigerian landscape that resemble data protection legislation like the Official Secrets Act, the Freedom of Information Act and the most recent NITDA Draft Guidelines for data protection with a view to show the adequacy or otherwise. The guidelines were examined in some detail. The paper summarily compares the present landscape with the European Union standard and concludes that Nigeria does not have adequate data protection legislation. The paper concludes that strong legislation is desirable to protect personal data in Nigeria.*

KEYWORDS: Data protection, legislation, guidelines, cyberspace, security.

INTRODUCTION

Quite a few Nigerians have expressed concern about the lack of data protection legislation in Nigeria[1]. As a developing economy that is eager to be placed on the same map with the economically advanced nations of the world, the realities on ground mandate that as a nation, Nigeria should have adequate legislation to protect information especially in the terrain of electronic commercial transactions. Till date, Nigeria does not have any data protection legislation that is comparable to that in operation in other countries like South Africa, India, the United States,

*LL.B. (Hons) B.L., LL.M, Ph.D., Lecturer, Faculty of Law, Ekiti State University, Ado-Ekiti.
**LL.B. (Hons) B.L., LL.M, MPA, M.Phil., Ph.D., Professor & Dean, Faculty of Law, Ekiti State University.

1 Bisi Olaleye *The Sun* 'Is Data Protection Act inconsequential?' Tuesday, 22nd March, 2011 available at http://www.sunnewsonline.com/webpages/features/suntech/2011/mar/22/suntech-22-03-2011-001.htm; Franklin Akinsuyi, "Data Protection Legislation for Nigeria: The time is Now!" available at http://techtrendsng.com/data-protection-legislation-for-nigeria-the-time-is-now-part-1/ ; See also Tayo Ajakaye, "Nigeria: Data protection, Storage, E-Government and Nigerians" Thisday, 27th April, 2005. Also available at http://allafrica.com/stories/200504280219.html ; Ayo 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 95/56" Information and Communications Technology Law, Volume 16 (No 2) 2007; Izuogu, Chukwuyere Ebere, "Data Protection and other Implications in the ongoing SIM Card Registration Process" available in electronic form at http://ssrn.com/abstract=1597665 accessed on 15th February, 2012

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

Canada, countries in the European Union or other developed nations. As a matter of fact, there is no federal or state enactment or legislation that has the protection of personal data as its main object within the Nigerian legislative framework.

The closest that Nigeria has to a data protection legislation is the Draft Guidelines on Data Protection published by the National Information Technology Development Agency.[2] It is interesting to note that a cursory look at the draft guidelines show that it is not more than it claims to be, "draft guidelines" with little or nothing to show legislative authority or thoughtfulness. However, this paper will attempt to look at some of the laws in Nigerian statute books that offer some measure of protection to information and some legislative attempts in the forms of bills before the National Assembly and the NITDA Draft Regulations before attempting to show the adequacy or otherwise of those laws.

LEGISLATIONS FOR CYBERSPACE

It is important to state at the onset that most countries that have legislations for data protection have earlier taken steps to legislate for some other foundational aspects of interactions in cyberspace. For instance the United Kingdom has the Computer Misuse Act 1990 which was designed and enacted before the 1998 Data Protection Act. Countries[3] have over the years found the need to legislate for the emerging trends from information communication technology due to the understanding that ordinary laws made for regular offline interactions are not adequate to tackle the challenges of the online world.

Even though, as is generally known, the 1999 Constitution of the Federal Republic of Nigeria guarantees the protection of the privacy of every citizen, that is how far as it goes. Interestingly, the second schedule to the Constitution that deals with legislative powers does not mention anything like information communication technology directly. An abstraction or inference may only be made from some clauses that govern matters like posts, telegraphs and telephones[4]; trade and commerce[5]; wireless, broadcasting and television[6]. But it appears that any legislation that may be made on this area lies within the legislative competence of the National Assembly and not that of the states. The fact that cyberspace lies outside the reach of sovereign nations ordinarily, precludes any component state in the Nigerian federation from attempting to legislate on it.

Previous Attempts at Legislation

Several bills have been drafted that should have addressed areas bothering on information communication technology in Nigeria, but till date, none of them has been passed into law. Some

[2] Clause 1.2 of the Guidelines claims that the authority for the Regulations is in accordance with the NITDA Act 2007. The provision states further that the regulations are specifically issued pursuant to Sections 6, 17 and 18 of the NITDA Act and is subject to periodic review by the NITDA.
[3] Example include countries like Belgium, France, Luxembourg, Germany, Sweden, Switzerland, Romania, Canada, The United States of America, Malaysia, Singapore and the ESCWA member countries like: Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, the Syrian Arab Republic, the United Arab Emirates and Yemen.
[4] Second Schedule Part 1, item 46
[5] Second Schedule Part 1, Item 62
[6] Second Schedule Part 1, item 66

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

of the bills are: the Computer Security and Critical Information Infrastructure Protection Bill 2005,[7] the Cyber Security and Data Protection Agency (Establishment, etc) Bill 2008[8] the Electronic Fraud Prohibition Bill 2008,[9] the Nigeria Computer Security and Protection Agency Bill 2009,[10] the Computer Misuse Bill 2009,[11] and the Economic and Financial Crimes Commission Act (Amendment) Bill 2010.[12]

Two major enactments that may be examined in the course of this paper as dealing with information are the Official Secrets Act[13] and the Freedom of Information Act[14]. These two enactments appear to have some protection for personal information. It shall be examined whether they qualify for data protection legislation or not. One will thereafter look at the draft Computer Security and Critical Information Infrastructure Bill, and the National Information Technology Development Agency Draft Guidelines on Data Protection.

The Official Secrets Act

This enactment is a relic of the colonial administration[15]. It was designed as an Act to make further provision for securing public safety; and for purposes connected therewith. Of the nine sections of the Act, one feels only two bear some (if any) relevance to the issue at hand. Section 1 provides for the 'Protection of official information, etc' and states that:

(1) Subject to subsection (3) of this section, a person who –
- (a) Transmits any classified matter to a person to whom he is not authorised on behalf of the government to transmit it; or
- (b) Obtains, reproduces or retains any classified matter which he is not authorised on behalf of the government to obtain, reproduce or retain, as the case may be,

is guilty of an offence.

(2) A public officer who fails to comply with any instructions given to him on behalf of the government as to the safeguarding of any classified matter which by virtue of his office is obtained by him or under his control is guilty of an offence.

(3) In proceedings for an offence under subsection (1) of this section relating to any classified matter, it shall be a defence to prove that –

(a) when the accused transmitted, obtained, reproduced or retained the matter as the case may be, he did not know and could not reasonably have been expected to believe that it was a classified matter; and

(b) when he knew or could reasonably have been expected to believe that the matter was classified matter, he forthwith placed his knowledge of the case at the disposal of the Nigerian Police Force.

Section 4 of the Act provides for the control of mail forwarding agencies. It states that:

[7] Sponsored by the Executive
[8] Sponsored by Hon. Bassey Etim
[9] Sponsored by Senator Ayo Arise
[10] Another Executive Bill
[11] sponsored by Senator Wilson Ake
[12] Sponsored by Hon. Abubakar Shehu Bunu
[13] Cap 03, No 29 of 1962
[14] Of 2011
[15] It effectively replaced The Official Secrets Act of 1920 by the provision of Section 10 (3)

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

(1) The Minister may make regulations –
(a) For controlling the manner in which any person conducts any organization for receiving letters, telegrams, packages or other matter for delivery or forwarding to any other person; and
(b) Without prejudice to the generality of the foregoing paragraph, providing for the furnishing of information and the keeping of records by persons having or ceasing to have conduct of such an organization
(2) Regulations under this section may contain such incidental and supplementary provisions as the Ministers considers expedient for the purposes of regulations, including in particular provisions imposing penalties (not exceeding imprisonment for a term of three months or a fine of N100 or both) for any failure to comply with the regulations; and the regulations may make different provisions for different circumstances
(3) Regulations under this section shall; not come into force until they are approved by resolution of each House of the National Assembly.

It is important to note that the foregoing provisions clearly deal with official information or information belonging to or in the custody of the government. They do not in any way deal with information about private individuals in the custody of other individuals or other private organizations.

Secondly it deals with officials of the government mishandling information that is classified. Section 9 (1) of the Act explains 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'. Thus the only form or 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 misused by a person not in the employ of the government; such a person is not punishable or otherwise apprehensible by the provisions of this law. Thirdly, the law creates offences; it sees information purely as government asset that can only be protected against unauthorised disclosure and not as private assets for which damages or other form of compensation should be paid to the victim of such abuse. There is nothing in the whole law that offers protection to personal or private information.

The provisions of Section 4 on controlling of mail forwarding agencies seems to be enacted in a somewhat 'futuristic preparation' for Internet Service Providers or other agencies that handle electronic data and mail. The words "for controlling the manner in which any person conducts any organization for receiving letters, telegrams, packages or other matter for delivery or forwarding to any other person" would seem to cover any manner of information transfer whether in electronic form or physical form. But the reality of the present time demands more realistic and direct legislation for the protection of privacy rights in the electronic sphere. One glaring shortcoming of the enactment is that it is penal in entirety, there are no provisions made for other remedies where individual informational rights are breached.

It seems the original intention of the lawmakers when this law was enacted was solely to prevent information about acts of government from getting to private hands. Over the years, this very Act has been used to prevent the citizens from knowing what transpired in government circles as every

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

request for information by the citizenry was met with a stonewall in the name of the Official Secrets Act. The democratization of the Nigerian government and the return to civil rule in 1999 stirred a fresh move to have acts of government made known or discoverable to the people hence the clamour for the Freedom of Information Act which dragged on till it was enacted in 2011.

The Freedom of Information Act

This statute was enacted in 2011 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". It seems the intendment of this Act is to give the liberty to access public information which the Official Secrets Act hitherto withheld from Nigerians. Again, similar to the Official Secrets Act, the Freedom of Information Act deals with information in the custody of public institutions. However, there is an inherent and natural conflict between the right of privacy on the one hand and the right to know on the other. The reason for this potential conflict cannot be far-fetched: laws of data protection and privacy are primarily concerned with the restriction of disclosure of information, while freedom of information laws by design are meant to facilitate the general access to information.

However, it is worth pointing out here that the Act only deals with access to public nature information. The Act cannot be taken as data protection legislation by any standards, as the provisions are not comparable to what the European Community Data Protection Directive mandates member states to consider in legislating for data protection. Firstly, the provisions of the Act do not manifest the eight core data protection principle that have evolved overtime and which have become the bedrock of data protection legislation around the world and which have been given international significance by the Data Protection Directive. Every enactment across the globe that qualifies for data protection legislation embraces and revolves around those fundamental principles. Secondly, the Act does not make provision for any classification of information as private or public; it only talks about 'information that contains personal information'. Thirdly, the Act makes no reference to information in the custody of private organizations or individuals.

The crux of most data protection legislation in the present age has to do with preventing abuse of private information by private organizations. Countries like the United Kingdom that have a freedom of information law like Nigeria, realized the difference between the two hence the enactment of separate data protection legislation. The only relevance that is worth pointing out is that information in public custody 'that contains personal information'[16] 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', there is no offence created and thus there is neither a penalty for such abuse nor a remedy for the party whose personal information is improperly or inappropriately disclosed.

[16] Section 15 (1) of the Freedom of Information Act, 2011

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

The Computer Security and Critical Information Infrastructure Bill

This Bill was first made public in 2005. The introductory part of the Bill describes its objectives among other things to "secure computer systems and networks and protect critical information infrastructure in Nigeria by prohibiting certain undesirable computer-based activities…" On a general plane, this Bill seeks to create legal liability and responsibility for modern global crimes carried on over a computer or computer systems forming a network, i.e. the internet. Some of these crimes, which carry penalties of fines ranging from the average sum of 100,000.00 (One Hundred Thousand Naira) to terms of imprisonment ranging on the average from six months imprisonment, include:[17] hacking and unlawful access to a computer or a computer network, spamming,[18] computer fraud, computer forgery, system interference, identity theft and impersonation on the internet, cyber-terrorism, cyber-squatting, misuse of computer for unlawful sexual purposes, etc.

The Bill requires every service provider to keep a record of all traffic and subscriber information on their computer networks for such a period as the President of the Federal Republic of Nigeria may by Federal Gazette, specify.[19] Service Providers are further required to record and retain any related content at the instance of any Law Enforcement Agency. It also allows any law enforcement agency in Nigeria, on the production of a warrant issued by a court of competent jurisdiction, to request a service provider to release any information in respect of communications within its network, and the service provider must comply with the terms of the warrant.

However, the Bill attempts to ensure the protection of the privacy and civil liberties of individuals by requiring that all communications released by a service provider shall only be used for legitimate purposes[20] authorized by the affected individual or by a court of competent jurisdiction or by other lawful authority. In furtherance of this, the Bill requires all law enforcement agencies carrying out their duties under it to have due regard[21] to the constitutional rights to freedom of privacy guaranteed under the 1999 Nigerian Constitution and take appropriate technological[22] and organizational measures to safeguard the confidentiality of the data retained, processed or retrieved for the purposes of law enforcement.

To ensure compliance by the service providers or body corporate, who are the providers of all form of telecommunication services in Nigeria and who are the processors of personal data, the Bill recommends that any breach of the provisions of the contemplated Law, by these persons, shall on conviction be liable to the payment of a fine of not less than N5Million.[23] In addition, each Director, Manager or Officer of the service provider shall be liable to a fine of not less than N500,000 or imprisonment for a term of not less than three years or to both the fine and the term

[17] Section 3 of this Bill makes it an offence for any person, without authority or in excess of such authority where it exist, to access any computer or access a computer for an unlawful purpose. It is also an offence for any person to disclose any password, access code or disclose any other means of access to any computer program without lawful authority.
[18] Spamming generally covers unsolicited emails and fraudulent emails
[19] Section 12
[20] This tends to accord with the 2nd data protection principle.
[21] Section 12(5)
[22] This also accords with the 7th data protection principle
[23] Section 12(7) of the Bill

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

of imprisonment. This singular provision makes the proposed law more penal in nature than protective.

However, the causes for concern that one has for the Bill are that: firstly there is no independent authority to monitor compliance with the provisions of the bill apart from the regular law enforcement agencies. It is not enough to stipulate penalties for non-compliance, there must be an appropriate machinery in place to ensure that private information are not abused in the course of data gathering for whatever purposes. Secondly, there is no provision for award of compensation where the data rights of individuals are violated. The imposition of higher monetary penalties may do well to enrich the coffers of the government but they do not in any way compensate for losses suffered when personal data is abused or misused.

Though the Bill attempts to provide for the security of data, it is not a clear-cut data protection legislation. A simple comparison between the Bill and European data protection legislation will show some clear defects or lacunae among others like:

1. No definition of what constitutes personal data
2. No identification of the right to privacy
3. No definition of what constitutes data subjects' rights
4. No appointment of a regulatory body to ensure compliance or redress breaches
5. No provisions for circumstances where data can be used without the consent of the data subject

Regardless of whatever effect it would have had on the protection of personal information, the non-passage of the Bill into law makes it nearly impossible and meaningless for this writer to discuss its effects and usefulness.

PRESENT DATA USAGE LANDSCAPE IN NIGERIA

It may be important to note that presently in Nigeria, personal information is more in demand and in use more than before. Some few years back, namely 2009, the Nigerian Communications Commission[24] directed all subscribers to GSM phone services to register their SIM[25] cards with the operators. Nobody, not even the members of the National Assembly raised the issue of a lack of a legislative framework for such an exercise. Thus millions of Nigerians willingly gave their personal data to companies that are largely foreign in origin with no guarantee that such data will not be open to abuse or that where abuse results, there will be adequate compensation to the victims.

As a developing economy, the level of internet penetration in Nigeria is rising. This is due to the technological developments evidenced in the availability of mobile phones that are capable of wide range internet operations. The days of restriction to computers that are connected via wired telephone lines or cybercafé operations alone are over as anybody within the comfort of his or her room can connect with the aid of modems or while on the go with internet enabled phones over cellular networks.

[24] The regulatory body overseeing telecommunication companies and their operations in Nigeria
[25] Subscribers Identity Module

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

As at 2012 Africa took 7% of the global internet usage statistics with a total of 167,335,676 users.[26] The degree of increase of internet users in Nigeria was staggering. With an estimated population of 170,123,740 people in 2012, and from an estimated 200,000 internet users in 2000, the number jumped to 55,930,391 in 2012 and Nigeria ranks as number 8 in the global ranking! The volume of Nigerian users on the popular social network site, Facebook, as at 2012 was found to be 6,630,200![27] The need for legislation for data protection in cyberspace is made more glaring with these statistics.

Further, the emergency of online trading companies like Konga,[28] Jumia,[29] Tafoo,[30] Dealdey,[31] Kaymu,[32] Buyright,[33] Mystore,[34] Circuitatlantic,[35] etc has compelled private individuals to release private information about themselves to these online stores. It is a basic outflow of e-commerce that the private information of the citizenry must of necessity get into other hands. But one way by which the advanced nations prevent abuse and damage is to enact appropriate legislation placing liabilities on data processors to ensure that personal information are secured and not unduly shared.

THE NITDA DRAFT GUIDELINES ON DATA PROTECTION 2013

The National Information Technology Development Agency Draft Guidelines on Data Protection was released by the agency in September 2013 as 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 of the Federal Republic of Nigeria. The guidelines are purportedly issued pursuant to Sections 6, 17 and 18 of the NITDA Act and a breach of the guidelines is deemed to be a breach of the Act. The guidelines further provide that it shall be subject to periodic review by the agency while it permits additional data protection and security guidelines to be developed and used at organisation discretion in accordance with the rules.

Provisions of the NITDA Act on Data Protection

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. Since the Data Protection Guidelines issued by the NITDA purports to be issued pursuant to the provisions of Sections 6, 17 and 18 of the Act, it may be necessary to look at the provisions albeit summarily. Section 6 of the Act deals with the functions of the agency and states 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

[26] http://www.internetworldstats.com/stats1.htm Accessed on 26 March 2014
[27] http://www.statisticbrain.com/africa-internet-user-statistics/ accessed on 26th March 2014
[28] www.konga.com,
[29] www.jumia.com.ng
[30] www.tafoo.com
[31] www.dealdey.com
[32] www.kaymu.com.ng
[33] www.buyright.biz
[34] www.mystore.com.ng
[35] www.circuitatlantic.com

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

the use of electronic communication may improve the exchange of data and information. This is about the only paragraph in the whole of the section that has anything to say about data use or the protection thereof.

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. What role the Standards Organisation of Nigeria is to play in the protection of personal information online is left to the imagination of anyone. The remainder of the provisions in Section 18 states the penalty for any offence where no specific penalty is provided for in the Act.

It is difficult for anyone to see very strong links between the provisions of Sections 6, 17 and 18 of the NITDA Act and the other legislations for data protection that are in operation in other countries. As a matter of fact, it is not easy by any stretch of imagination to see any section of the NITDA Act that directly or indirectly empowers the agency to engage in any form or type of lawmaking for data protection in Nigeria. Data protection legislation is a form of human right protection legislation and it will amount to gainsaying to think all that is about data protection is just about technology and the need to develop its use or prevent the abuse thereof.

The NITDA Draft Guidelines

The preamble to the National Information Technology Development Agency Draft Guidelines on Data Protection alludes 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. It 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 strange thing that beclouds knowledge is that how the agency came about this is not stated.

The Draft Guidelines are divided into three main sections. Section one covers matters like the preamble, the authority on which the guidelines are based, the scope and application of the guidelines, the purpose and definition of terms. Section two covers aspects like guidelines for data protection, guidelines for data processing, guidelines for data access and guidelines for data security officers. Section three outlines data protection guidelines principles which are in *pari materia* with the data protection principles enunciated in the European Data Protection Directive and which have been incorporated into the various data protection laws of other nations that have legislated on the same.

The NITDA Draft Guidelines specifically states that its purpose[36] is to prescribe guidelines for all organizations or persons that control, collect, store and process personal data of Nigeria residents within and outside Nigeria for the protection of Personal Data or Object Identifiable Information (OII) and to prescribe minimum data protection requirements for the collection, storage, processing, management, operation and technical controls for personal information.

[36] Section 1.5 of the Data Protection Guidelines

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

In delimiting its own scope, the guidelines shall cover the processing of personal data whether by automatic or by other means where they form part of a filing system, it will also cover data controllers or processors operating within Nigeria or processors outside Nigeria if they process personal data of Nigerian residents.

Though the guidelines stipulates that it shall apply to all data processors whether in the public or private sector, it does not cover the processing of personal data processing operations concerning public security, defense, national security and the activities of the nation in areas of criminal law.

Guidelines for Data Collection

The Guidelines set out to separate the actual collection of data from its processing. There does not appear to be any need for this and it does not look like an innovation because it is virtually impossible to collect personal data in the electronic world without some sort of processing. These are contained in Section 2 of the draft guidelines and the summary of the whole provisions is no different from the provisions of Section 2 of the United Kingdom Data Protection Act of 1998.

The guidelines places the responsibility for the protection of the privacy of natural persons on Data controllers who are natural or legal persons, public authority, agency or any other body which alone or jointly with others determine the purposes or means of processing personal data.[37]

Secondly, 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.[38]

Thirdly, 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 fourth guideline deals with transfer of personal data which are undergoing processing (or which are intended to be processed after transfer) to another country. This is only permitted where the country in question ensures an adequate level of protection.

[37] Section 2.1.1 of the Guidelines. The data controllers are to secure this privacy in accordance with the guidelines and the provisions and prescriptions of Section 5, Part 1 and Part 2 of the National Information Systems and Network Security Standards and Guidelines.

[38] 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.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

The fifth provision under these guidelines gives data controllers a moratorium of 12 months from the data of adoption of these guidelines, within which to bring directives and administrative provisions necessary to comply with them. The import of this is that companies processing data are not under any serious legal duty to conform or comply with the provisions of the guidelines until same are adopted.

The last guideline for data collection requires organizations to implement effective privacy policies and procedures and state those policies both online and offline in order to ensure that Nigerian people understand and have confidence in the proper use and safety of personal information.

As has been pointed out earlier, these are just guidelines. How effective these will be in a country like Nigeria where the average business entity is eager to find ways to circumvent legislation will be revealed with time. It is common knowledge in Nigeria that telecommunication companies do not respect the privacy of the citizenry going by the volume of unsolicited text messages that are sent into subscribers' phones daily. If legislations are not taken seriously, then what level of seriousness will be attached to regulations?

Data Protection Guidelines Principle

The last segment of the Draft Guidelines attempts to state a set of principles that undergird the Data Protection Guidelines. The provisions are set out hereunder:

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 bedrock of all data protection legislation. From the European Data Protection Directive to the data protection laws of countries like Malaysia, South Africa, India and others, the above principles are enshrined firmly.

A CRITIQUE OF THE NITDA DRAFT GUIDELINES

One must as a matter of sincerity commend the National Information Technology Development Agency for taking the bull by the horns and making a fair attempt at doing the work of the National Assembly. The Nigerian constitution expressly provides that the legislative power of the Federal Republic of Nigeria shall be vested in the National Assembly. But it seems the Nigerian National Assembly has not considered the core issue of data protection in the online environment worthy of legislative attention. One makes the assertion because of the several issues raised[39] and moves

[39] Akinsuyi and others have at various times raised the urgency of data protection legislation for Nigeria

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

earlier made[40] by researchers and others alike and the fact that the Nigerian lawmakers cannot claim to be oblivious of the serious need for a national legislation in this regard.

However, one feels that the NITDA Draft Guidelines are not strong enough to bear the weighty demands of a proper data protection legislation. A close look at the draft guidelines as shown in the published document shows a clear lack of definite legislative creativity. The arrangement of the sections and the content of the articles do not present a really serious effort on the part of the draftsman. The whole document appears to be a hurriedly drafted work or a copied document. Section 3 of the Draft Guidelines which is titled 'Data Protection Guidelines Principles' says the eight principles are guidelines for best practice in handling personal data and goes ahead to outline the principles accompanied with explanatory notes that seem to trivialize the importance of the document as a regulatory document. It is important to restate here that the eight principles are not just best practices for handling personal data but the real backbone of all legislative efforts in regulating data protection.

Secondly, the document does not create legal rights for data subjects though it attempts to create liabilities for organizations that process data. For example, 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 thereto. 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 entitles to receive compensation from the controller for the damage suffered'. But the guidelines do not say more. The procedure to be followed in this instance is not discussed and mode of assessing the amount of compensation payable is not known. Moreover, where the offending party that was involved in unlawful processing fails to pay the compensation, there is not much that the victim can do.

Thirdly the mechanism for enforceability is not clearly stated in the regulations. Standard enactments in the field of data protection across the world also establish mechanisms for enforcement due to the propensity or tendency of data controllers to process data at great risks to data subjects. The various data protection legislations of the advanced economies and other developing jurisdictions created specific mechanisms or institutional frameworks for data protection.[41] One considers it a gross omission for any data protection regulation to be left without specific institutional enforcement mechanism. The National Information Technology Development Agency that released the draft guidelines did not arrogate to itself the power to enforce the provisions of these guidelines. The possibility of abuse of personal data in the face of such lapse is still very strong especially in a society like Nigeria.

Fourthly, the draft guidelines are not to come into operation until they have been adopted. The document fails to tell who is responsible for the adoption and when the adoption will take place. Placing such a matter as important as data protection in abeyance is tantamount to not making any

[40] Various people at various times have moved for some bills to become law in this area
[41] 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.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

legislative effort at all. As it is now, the draft guidelines are not more than a draft. They have no operative effect.

Guidelines by nature are two-sided documents. It is largely a set of dos and don'ts that one party gives to another. It is not very much like an enforceable social contract similar to a legislation that creates rights and liabilities. At best it gives a set of expectations that one has from the other and hardly is a third party allowed to claim any breaches thereby. It is the regulatory agency that may impose sanctions where there are breaches of the regulations. Even at that, the draft guidelines look more like a set of advisory principle that data processors are expected to follow with no coercive sanction or threat of punishment where the guidelines are violated.

The NITDA itself is a creation of statute with limited powers. Though it may try to fill in some gaps in attempting to fulfill its roles, the present global trend in the protection of individual online privacy in cyberspace demands real legislative enactments to strengthen data protection regulations. The subject of data protection as shown in the course of these research work is much more important what should be the subject of delegated legislation. It is the considered opinion of this writer that the draft guidelines should be polished into the form of an appropriate legislative bill and same should be presented to the National Assembly for enactment.

NIGERIAN DATA PROTECTION PRACTICE (?) AND THE EU DATA PROTECTION PRACTICE

From the foregoing it is clear that there is presently no legislative enactment in force that is designed specifically to govern data protection in Nigeria. Where somebody living in Nigeria feels his informational privacy rights have been violated or breached, the only main remedy opened 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[42]. Typically, 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 torts mentioned above.

Private nuisance may be seen to have some remedies in data protection. In the Canadian case of *Motherwell v. Motherwell*[43] and the English case of *Khorasandjian v Bush*[44] it was used to provide remedies for unwanted mail and unwanted phone calls respectively. But then private nuisance is a tort against the enjoyment of land and it has been held[45] by the English Court that a person must have an interest in land before he can have the standing to sue. Thus in this age of mobile communications, the usefulness of this common law action is limited. 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.

[42] Vili Lehdonvirta, (2004) "European Union Data Protection Directive: Adequacy of Data Protection in Singapore" Singapore Journal of legal Studies, 511-546
[43] (1976) 73 D.L.R. 62.
[44] [1993] 3 All E.R. 669
[45] *Hunter v Canary Wharf Ltd*. [1997] 2 All E.R. 426

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

But then truth is a complete defence to defamation, whereas in the law of data protection, the veracity or authenticity of information about a person is not the issue, but that one wants to keep it private.

The law of confidence remains the main way by which misuse of confidential information may be curtailed under these circumstances[46]. This remedy seems appropriate from the viewpoint of data protection. In the English case of *Douglas & Others v Hello! Ltd. and Others (No 3)*[47] the claimant was awarded damages under both breach of confidence as well as the United Kingdom Data Protection Act 1998. However, as Megan Richardson[48] points out, the doctrine has evolved to respond to privacy issues such as the case in question, but it remained centred around the concept of publication. Despite 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.[49]

The foregoing discussion shows that common law has been seen to be inadequate otherwise there would be no need for European nations to design a whole new legal regime for data protection. The advent of modern technology and the methods of doing business in the present dispensation demand laws that are responsive to the challenges of the times. Of all the bills discussed above that appear to have bearing to information communication technology related matters, none of them appears to have embraced the data protection principles enshrined in the European Convention[50] or the Data Protection Directive[51].

The resultant effect of this is that 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. Since only a small percentage of countries across the globe have been found to have adequate levels of protection, there must be found alternative mechanisms to legitimise data transfer to the rest of the world. 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

[46] Megan Richardson, "The Private Life After *Douglas v. Hello!* (2003) Sing. J.L.S. 311 at 327
[47] [2003] All E.R. 996
[48] *Ibid* note 25 above.
[49] *Ibid*
[50] Convention for the Protection of Individuals with regard to Automatic Processing of Data, European Treaty Series No. 108, Strasbourg 1981. http://www.coe.fr/eng/legaltxt/108e.htm
[51] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

(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".

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". There is no need for fear of conflict between national laws as the aim of the Directive is the harmonisation of national legislations.

The second way is where Nigeria as a country is granted similar privilege as is granted the United States under the Safe Harbour Principles. 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 does not go well with the 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[52]. However, no one is sure if any European country will be willing to offer Nigeria

[52] 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

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

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 and the OECD Guidelines on the Protection of Privacy and Transborder 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 transborder flow of data'.[53] As our laws presently stand, Nigeria has no basis for desiring to have the data of European citizens processed in the country. A consequent loss arising from this is that software contracts which are been outsourced to other nations like India may not be given to any Nigerian company.

CONCLUSION

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 not capable of being 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. It is the strong opinion of this writer that adequate legislation is needed for data protection in Nigeria.

REFERENCES

Ajakaye, T. (2005) "Nigeria: Data protection, Storage, E-Government and Nigerians" Thisday, 27th April,. Also available at http://allafrica.com/stories/200504280219.html ;

Akinsuyi, F. F., "Data Protection Legislation for Nigeria: The time is Now!" available at http://techtrendsng.com/data-protection-legislation-for-nigeria-the-time-is-now-part-1/ ;

Izuogu, C. E., (2012 "Data Protection and other Implications in the ongoing SIM Card Registration Process" available in electronic form at http://ssrn.com/abstract=1597665 accessed on 15th February,

Kobrin, S. J., (2004), "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

Kusamotu, A. (2007); "Privacy Law and Technology in Nigeria: The Legal Framework will not meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/56" Information and Communications Technology Law, Volume 16 (No 2)

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

Olaleye, B. (2011) *The Sun* 'Is Data Protection Act inconsequential?' Tuesday, 22nd March, available at http://www.sunnewsonline.com/webpages/features/suntech/2011/mar/22/suntech-22-03-2011-001.htm;

Richardson, M., (2003) "The Private Life After *Douglas v. Hello!* Sing. J.L.S. 311 at 327

[53] The Preamble to the OECD Guidelines on the Protection of privacy and Transborder Flows of Personal Data. Full text available at http://www.oecd.org.document

ISSN 2053-6321(Print), ISSN 2053-6593(Online)