Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms

Lukman Adebisi Abdulrauf[*] and **Charles Manga Fombad**[**]

Abstract The right to personal data protection is, without doubt, an important right in the jurisprudence of rights in the contemporary information society. It is becoming as crucial as other orthodox human rights and also attracting significant attention from academics, lawyers, human rights activists and policy makers. In spite of the growing attention data protection receives at international and regional levels, Nigeria is still lagging behind many competitor states like South Africa in establishing an effective legal framework to protect personal data. Individuals' personal data is being collected and used without any serious form of control to check against abuse. This paper reflects on opportunities, option and challenges to legal reforms on data protection in Nigeria. It contends that certain legislative and practical challenges stand in the way of an effective legal regime on personal data protection. The paper suggests appropriate legal reforms that are needed to enable prevent the increasing risks of violating the right to data protection in a country that is making rapid advances in Information and Communication Technology but hamstrung by an outdated regulatory framework.

Keywords: personal data, data protection, data protection law, the right to data protection, legal reforms, Nigeria

Introduction

Data protection is a global issue and a topic of concern to various actors. It is constantly under attack by states and commercial entities that indiscriminately accumulate and use individuals' personal data in violation of their human rights. The proliferation of personal data globally has several benefits, yet it exposes individuals to certain risks like making them more transparent and subjecting them to various indiscretions of states and business entities like using such information for purposes other than that which there were collected and exposing individuals to risks resulting from inadequate security safeguards for information legitimately collected. Indiscriminate personal data processing could also increase information and power asymmetries between the people and these institutions (state and business entities).[1] These are all issues brought about as a result of the growing demand for personal data in the globalised and digital age.[2] To address some of the concerns, the law on data protection establishes certain principles regulating the collection, use and disclosure of individuals' personal data so as to protect their human rights to dignity, autonomy, personality, and as we will argue shortly, data protection. The essence of these regulations is not to prohibit the processing of personal data as this may be practically impossible in the globalised world but rather regulate its proper use.[3] Personal data may be collected and used provided it is done in a rights-respecting manner. In this case,

[*] Department of Public Law, Faculty of Law, University of Ilorin, Nigeria. E-mail: lukmanrauf@gmail.com

[**] Professor of Law, Institute for International and Comparative Law in Africa, Faculty of Law, University of Pretoria, South Africa.

1 Lynskey (2014:592).

2 See generally Kuner (2013:1); Lagos (2014:187).

3 De Hert and Gutwirth (2009: 3).

provided the individual subject of the personal data has substantial control over its accumulation and use, then personal data may be freely used for various purposes. Thus, data protection law essentially protects individuals from intrusive governments and companies.[4]

Nigeria has the largest economy and population in Africa.[5] It is fast becoming one of the most attractive countries to invest in on the African continent. The country has progressively embraced information technology across all its major sectors. There is also a gradual recognition of the benefits of personal information and the need for its harmonisation for ease of access and use. For example, the Nigerian President recently called on the key government agencies that collect and use biometric data to "harmonize the collection and usage of biometric data in the country" so as to prevent replication of effort and ease exploitation.[6] Similarly, the Nigerian government is at an advanced stage in creating a comprehensive database of vehicle owners in the country so as to facilitate crime detection.[7] All these have the effect of increasing the volume of personal information available. As laudable as these initiatives may be, they certainly come with some cost to individuals, especially in the absence of a coherent legal/policy framework on data protection. Many people are prone to risks such as abuse and misuse of their personal information resulting from possible data breaches and discrimination. In the event any of these happens, individuals are also left without adequate legal remedies. These reasons and many more justify the need for a more serious debate on data protection at this point in Nigeria's history.

It is against this backdrop that this paper reflects on opportunities, options and challenges to legal reforms on data protection in Nigeria. The article is divided into 5 parts. Part II establishes the place of data protection in modern Nigeria. This is done by briefly identifying a number of legal issues in the country which provoke discussions on the need for data protection law. Flowing from this, part III considers the legal framework for data protection. In this part, we unpack the concept of data protection and consider the vexed issue of its human rights status. There is also an analysis of the extant legal framework on data protection. It is contended that the existing legal framework in Nigeria may not withstand the diverse challenges of personal data protection. Part IV looks at two issues. First, we examine attempts to develop a legal framework of data protection in Nigeria. Here, we analyse the draft bills on data protection in the country with a view to showing how opportunities for legal reforms have been utilised by policy makers in Nigeria. Second, we analyse the weaknesses of the draft bills and the entire legal framework of data protection in the country. Based on this, part V considers the future of data protection in Nigeria. We provide our thoughts on practical ways in which proper legal (and other) reforms can be carried out to enhance data protection. We conclude the paper in Part VI with our thoughts on the future of data protection in the country.

---

4 Van der Sloot (2015:26).

5 According to Nigerian Statistic Office, Nigeria's GDP for the year 2013 is 80.3 trillion naira (£307.6bn: $509.9bn). This surpasses that of South Africa at the end of 2013. Its population is estimated to be about 170 million people which is three times larger than South Africa's population. Economists however argue that these are mere figures as Nigeria's economic output is underperforming. See 'Nigeria becomes Africa's biggest economy' *BBC News Business*, 6 April 2014, available at http://www.bbc.com/news/business-26913497.

6 The key agencies include National Population Commission (NPC), National Identity Management Commission (NIMC), Federal Road Safety Commission (FRSC), Independent National Electoral Commission (INEC) National Population Commission, National Identity Management Commission, Federal Road Safety Commission, Independent National Electoral Commission." Buhari charges NPC, NIMC, FRSC others to harmonize biometric data" http://dailypost.ng/2015/08/10/buhari-charges-npc-nimc-inec-frsc-others-to-harmonize-biometric-data/ accessed 30 October 2016.

7 See V Ekwealor "The Nigerian Government is building a database of vehicle owners; it is not looking promising" https://techpoint.ng/2016/07/12/database-vehicle-owners-nigeria/ accessed 30 October 2016.

The Place of Data Protection in Modern Nigeria

Issues of data protection and the level of technological development in a society usually go hand in hand, thus a discussion on data protection is better appreciated when situated within the context of IT penetration. We must however state that though advances in IT has increased the need for data protection, individuals' personal information are still exposed to risks when they are manually processed. That notwithstanding, computerised processing generates more risks than manual processing especially for developing countries, like Nigeria, without proper legal frameworks and that is a reason why it is the focus of this discussion. .

Globalisation and e-commerce has resulted in the improvement of IT infrastructure in Nigeria. This fact is noticeable in the level of internet and telecommunication penetration in the country. Recent statistics show that the level of internet penetration[8] in the country is around 40% with about 70 million internet users making Nigeria the eighth largest internet user in the world.[9] This is a significant leap from about 10 years ago.[10] Similarly, the government is making more efforts towards enhancing this infrastructure by improving its broadband facilities.[11] Telecommunications have also drastically improved within the last few years with about 87% penetration.[12]

The forgoing has led to an upsurge in data protection issues in the country. First, improved technological infrastructure has enhanced government surveillance activities with the capability to accumulate large amount of individuals' personal data which may sometimes be inaccurate.[13] Similarly, various government institutions are improving their database facilities which raises questions regarding accountability and security safeguards of personal data in these databases. Second, private commercial entities, having recognised the importance of personal

---

8 Internet penetration is 'the portion of the population that has access to the internet. It defines a portion of the digital divide.' Ahn and McNutt (2015:55).

9 Ranked after countries like China, United States (US), India, Japan, Brazil, Russia and Germany who are ranked 1st -7th respectively. See Internet Live Stat 'Nigeria internet user' available at http://www.internetlivestats.com/internet-users/nigeria/ (accessed 20 January 2015). The figures are based on an elaboration of data by the International Telecommunication Union (ITU), World Bank, and United Nations Population Division. See also Internet World Stats "Usage and population statistics" http://www.internetworldstats.com/stats1.htm accessed 20 January 2015. There are inconsistencies in figures by both sources however the difference is not substantial.

10 Where Nigeria was ranked 20th largest internet user in the world. Ibid.

11 "Nigeria's National Broadband Plan 2013-2018" a submission by the presidential committee on broadband http://www.researchictafrica.net/countries/nigeria/Nigeria_National_Broadband_Plan_2013-2018.pdf accessed 20 January 2015 p.12. In the document, broadband is used to refer to high speed communication networks that connect end-users at a data transfer speed greater than 256 Kbit/s. The term is currently used in a way that is reflective of a user's experience thus 'broadband within the Nigerian context is defined as an internet experience where the user can access the most demanding content in real time at a minimum speed of 1.5Mbit/s.'

12 As of September 2014, the total number of active mobile telephone lines was estimated to be over 130 million which is about 87% penetration, as against less than 1% in the year 2000. See "Subscriber Statistics: Monthly Subscriber Data" Nigerian Communications Commission http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:art-statistics-subscriber-data&catid=65:cat-web-statistics&Itemid=73 accessed 20 January 2015.

13 For example, *Premium Times*, a Nigerian media outlet, recently reported increasing surveillance activities by the Nigerian government. See M. Mojeed, "EXCLUSIVE: Nigerians Beware! Jonathan procures N11 billion equipment to tap your phones", *Premium Times* (Nigeria), 26 February 2015 http://www.premiumtimesng.com/news/headlines/177557-exclusive-nigerians-beware-jonathan-procures-n11-billion-equipment-to-tap-your-phones.html accessed 28 February 2015.

data in a globalised world, also engage in its indiscriminate accumulation for commercial gains. This fact is underscored in the recent activities of commercial banks,[14] retail outlets[15] and credit bureaus.[16] The activities of these private and public entities pose a number of legal challenges for individuals. First, personal data is not collected fairly and lawfully in many cases. Second, questions arise regarding accountability and security safeguard of personal data collected. Improper accountability and safeguard of this data exposes individuals to identity thefts and cyber-criminals. Third, accuracy of personal data in possession of these entities becomes an issue and may lead to unfavourable decisions against individuals based on this data and ultimately, discrimination. These issues depict the crucial place of data protection in modern Nigeria and question the legal mechanism for the protection of personal data.

Revisiting the Conceptual and Legal Framework of Personal Data Protection

Individuals' personal data is an embodiment of their personality which is under threat from the advances in technology. Their 'virtual personas' therefore require legal protection. Three issues will be briefly examined here. First, an attempt will be made to determine the nature and ambit of data protection law. Second, the contemporary debates on the status of data protection as a human right will be examined. Third, the scope of the law on data protection in Nigeria will be analysed.

Some reflections on the concept of data protection

Data protection laws essentially confer on individuals the right to personal data protection. This body of law partially owes its origin to data processing rules of northern European countries and the United States.[17] Principles of data protection were developed as a result of a realisation that the right to privacy was inadequate to protect individuals from the risks associated with large automated processing of data.[18] The term *data protection* is a German coinage *Datenschuz*.[19] According to De Hert and Gutwirth, data protection, though impossible to summarise in a few words, is a catch-all term for a series of ideas regarding the processing of personal data.[20]

---

14 Various activities of commercial banks in Nigeria raise data protection issues. They conduct Know-your customers (KYC) and gather large amount of customers' personal data. Recently, banks are required to conduct personal data verification through the Bank Verification Number (BVN) project. See "Central Bank of Nigeria introduces Bank Verification Number (BVN)" http://nairabrains.com/2014/10/central-bank-of-nigeria-introduces-bank-verification-number-bvn/ accessed 20 January 2015.

15 Retail outlets also engage in the collection and use of individuals' personal data through their various activities. For example, there are calls to intensify direct marketing practices in Nigeria. See "Direct Marketing Swallowing Conventional Marketing – IDMN Registrar" http://www.nigerianbestforum.com/generaltopics/direct-marketing-swallowing-conventional-marketing-%E2%80%93-idmn-registrar/ accessed 20 January 2015.

16 See "Credit Bureau Association of Nigeria" http://www.mfw4a.org/news/news-details/article/2869/credit-bureau-association-of-nigeria.html -accessed 20 January 2015).

17 These rules are generally called the Fair Information Practice Principles (FIPPs). Modern data protection law is built around these principles which were broad, aspirational, and included a blend of substantive and procedural principles. See Cate (2006:341).

18 Van der Sloot (2014: 307). See also Birnhack (2008: 509).

19 Bygrave stated that *Datenschutz* is in turn derived from the notions of *Datensicherung* and *Datensicherheit* meaning 'data security'. Bygrave (2002: 22).

20 De Hert and Gutwirth (2009:3).

Governments apply these series of ideas to reconcile fundamental but conflicting values such as privacy, free flow of information and the need for government surveillance.[21] In a more succinct form, Roos describes data protection as, 'a set of measures aimed at safeguarding individuals (data subjects) from [the] harm resulting from the computerised or manual processing of their personal information by data controllers.'[22] These measures comprise of a group of principles on the processing of personal information usually called the 'Fair Information Practice Principles (FIPPs)'.[23]

The forgoing shows that data protection laws regulate almost all or most stages in the *processing* of certain kinds of data.[24] The word 'processing' within the scheme of data protection is an 'operation or set of operations performed upon personal data, whether or not by automatic means.'[25] Such operation includes *inter alia,* collection, recording, adaptation or alteration, disclosure, dissemination, locking and erasure.[26] In fact, Kuner opines that 'it is difficult to conceive of any operation performed on personal data in electronic commerce which would not be covered by it [processing]'.[27] It is important to note that not all data/information[28] fall within the ambit of data protection law.[29] For data to be protected, such data must be 'personal data' which is data that relates to or identifies (or likely to identify) a natural person.[30] In some jurisdictions, personal data also includes information that identifies a legal person or collective legal entities.[31] Furthermore, personal data within the context of data protection does not

---

21 Ibid.

22 Roos (2008:313).

23 Ibid.

24 Bygrave (2014:1); See also Bygrave (2002:1).

25 European Union Data Protection Directive 95/46/EC of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data 1995 (EU Directive) http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046 accessed 23 February 2015 Article 2.

26 Ibid, see also Protection of Personal Information (POPI) Act, No 4, 2013 of South Africa, http://www.justice.gov.za/legislation/acts/2013-004.pdf accessed on 23 February 2015, Section 1 which defines processing in a similar light. This article will consistently make reference to this South African legislation because it is one of the most recent data protection legislation and it arguable is a representation of a modern data protection piece of legislation.

27 Kuner (2007: 74). Many laws and international codes on data protection however provide for exceptions relating to the processing of personal data for purely personal, artistic and journalistic purposes. See for example EU Directive, Section 3 and POPI Act, Article 7.

28 Both terms are used interchangeably in this paper even though a distinction can be drawn between them. According to Roos, data is unstructured or unorganised facts that need to be processed and organised to produce information. Information is thus a set of organised, structured and processed data. Roos (2008:313). Bygrave opines that 'it is artificial and unnecessarily pedantic…to maintain a division between the two notions, as such a division is usually difficult to maintain in practice.' Bygrave (2002:20).

29 Bygrave (2014: 1).

30 Example of personal data of natural persons within the scope data protection are identification number, email address, physical address, religion, race, gender, biometric information etc. See EU Directive, Article 2. See also POPI Act, section 1(b).

31 For example, POPI Act in Section 1 refers to 'existing juristic persons'. Bygrave made an elaborate discussion on the importance of data protection law for organised collective legal entities which is 'constituted on the basis of the individual members of the entity coming together to set up and maintain the entity through a series of more or less systematic, formalised measures.' There are two main categories of these entities, there are the legal/juristic persons and those that are not. The non-organised juristic persons are 'non-profit' organisations such as religious bodies. See generally Bygrave (2002: 173).

necessarily have to be secret or even private.[32] This fundamentally distinguishes the right to data protection from privacy.

The law on data protection therefore protects individuals (data subject)[33] from the harmful effects of the processing of their personal data by data controllers.[34] In Nigeria for example, a data protection law will help provide the required legal framework for the protection of information contained in databases of key government agencies and private entities. Some basic features of data protection law can be discerned from the foregoing discussions. First, data protection principles are usually contained in laws[35] which provide for basic principles of data processing, or the FIPPs.[36] The principles are at the heart of data protection and they run through all provisions of the law. The essence of these principles is to 'safeguard certain interests and rights of an individual when information on him/her is processed by others.'[37] These interests and rights, according to Bygrave, are 'expressed in terms of privacy, autonomy and/or integrity.'[38] Due to the complexities of processing of personal data and associated issues, a dedicated structure is established to oversee the implementation of substantive provisions of data protection legislation.[39] This is a second distinguishing feature and it requires the establishment of bodies generically referred to as Data Protection Authorities (DPA).[40] DPAs must function independently without interference from the state and various entities.[41]

We must state that certain diversities exist in data protection frameworks. This is largely because the key instruments that drive data protection at the international level vary in their approaches to certain issues. For example, the OECD Guidelines, which is one of the primary data protection international instruments is principle-based and non-binding. Likewise, it does not require a dedicated enforcement institution (DPAs). This is unlike the EU Directive (and Regulation) which is binding on member states of the EU and requires them to mandatorily establish DPAs. Most jurisdictions largely follow these two approaches (OECD and the EU). It may however seem that the approach of the EU is more influential and has gained more support from many countries especially in Africa.

---

32 Abdulrauf (2014:74). See also Bygrave (2002:42).

33 A data subject is an individual whom personal data relates. See POPI Act, Section 1. Protection of data subjects' interest is the primary aim of the law of data protection. 'Data subject' and 'Individual' will be used interchangeably in this paper.

34 A 'data controller', 'controller' and 'responsible party' all refers to the same person/entity. It means a natural or legal person or a public or private body who, alone or jointly with others, determines the purposes and means of processing of personal data. See EU Directive, Article 2 and POPI Act, Section 1.

35 Bygrave points out that "data protection laws often take the form of 'framework' laws. Instead of setting down in casuistic fashion detailed provisions on the processing of personal information, data protection laws tend to set down rather diffusely formulated, general rules for such processing and make specific allowance for the subsequent development of more detailed regulatory norms as the need arises." Bygrave (2002: 3).

36 Bygrave (2002: 2).

37 Ibid.

38 Ibid.

39 See for example EU Directive, Article 28 which requires member states to establish public authorities that will be responsible for monitoring the application of the directive.

40 Different terms are used by various data protection laws to denote the supervisory agency. For example, POPI Act, Section 39 uses 'Information Regulator'. In some other jurisdictions, like the UK and Canada, the office is centred on a particular public official usually called the privacy commissioner.

41 EU Directive, Article 28 (1); POPI Act, Section 39 (b). See also Greenleaf (2012:3-13): 3-13. See also Makulilo (2014: 847).

The above is not the only diversity that exists in data protection frameworks. Another salient, albeit highly controversial, feature of data protection which borders on diversity in approach is its status as a human right. We will now consider the issue.

Situating Data Protection as a Human Right: Examining the Contemporary Debates

There have been an intense debate on whether or not data protection can be classified as a human right. This debate is brought about as a result of its 'split personality'.[42] Across the world, data protection has been driven by human rights and economic values.[43] Thus, the controversy has always been which of the values should be predominant. The European Union's regime, which is a global pacesetter in data protection, [44] has immensely contributed to these controversies. This is because its approach to data protection oscillates between a 'market-making' tool and an instrument of human rights.[45] The approach of the OECD, on the other hand, is generally acknowledged purely to be pure commercial motivated. We will now examine the legal arguments on both sides so as to demonstrate what values should typically underpin a data protection regime and the implications for Nigeria.

A. Data Protection as an Economic Issue[46]

Several arguments are proffered in support of the claim that data protection is strictly a commercial issue. Without a doubt, one of the initial motivations for the law on data protection was for the purpose of enhancing Transborder Data Flows (TBDF). This is as a result of the growing profile of personal data as a commodity that was increasing needed across borders. Bygrave notes that the fear of disrupted data flows probably had the most significant influence in stimulating the adoption of international data protection instruments, especially the Organisation for Economic Cooperation and Development (OECD) Guidelines[47] and the EU Directive.[48]Another commercially motivated argument for data protection is economic protectionism. Countries, especially those under treaty obligation to reducing tariff barriers, fear that other countries may use national data protection laws as a non-tariff barrier.[49] Similarly, there were fears that 'in the absence of data privacy laws, the general populace will lack the confidence to participate in commerce, particularly as consumers/prosumers.'[50] In addition, there is a gulf between countries that view data protection from an economic perspective, like the US[51]

---

42 Lynskey used the term 'spilt personality' in this context to denote the dual objectives of data protection. Lynskey (2013: 59).

43 Makulilo (2014: 846).

44 Levin and Nicholson (2005: 374).

45 Lynskey (2013).

46 We use the term 'economic' and 'commercial' interchangeably in this paper to depict a business driven or profit-making agenda or motive.

47 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal data, available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm accessed 23 February 2015.

48 Bygrave (2014: 11).

49 Caruana and Cannataci (2007: 104).

50 Bygrave(2014: 11).

51 See Craig and Ludloff (2011: 68), who contend that the US treats data privacy as a commodity that can be bought and sold. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) has also been argued to be driven by purely economic sentiments. Berzins (2001-2002: 609-645).

and those that see data privacy as deeply rooted in human rights, like member states of the EU.[52] The EU Directive also gives so much credence to the fact that data protection is economic in nature as it places so much emphasis on the EU's establishment of internal market objective.[53] Gutwirth's sharp criticism of the EU data protection regime is apt with regard to its commercial agenda where he argued that '[t]he European Midas is at work again: everything the Commission touches becomes a market.'[54]

B. Data Protection as a Human Right (Rights-based Approach)

Without ignoring the strengths of the arguments in favour of data protection as commercially driven, there is an equally stronger movement in favour of data protection as a human right. The contention is that anchoring data protection on economic success rather than human rights will naturally have the effect of relegating privacy and autonomy to the background.[55] Thus, if a data protection instrument has pure economic motives, so much emphasis will be placed on regulating data flow at the expense of the individuals' human rights.[56] A rights-based approach will achieve the opposite as it anchors data protection on fundamental rights of data subjects.

In spite of the commercial purposes, there is no denying that data protection has its roots in the right to privacy in international human rights instruments like the Universal Declaration of Human Rights (UDHR),[57] International Covenant on Civil and Political Rights (ICCPR)[58] and European Convention on Human Rights (ECHR).[59] Thus, the normative basis of data protection is in human rights instruments which arguably makes it a human right too.[60] While some jurisdictions do not even distinguish privacy from data protection[61] others have anchored their data protection laws on the right to privacy.[62] The relationship between data protection and other human rights also strengthens the arguments in favour of it being a human right.[63] Apart from

---

52 Lloyd (2011:9).

53 A commentator pointed out that with regard to the EU Directive, its original purpose 'was not only to increase data privacy protection within the European Union, but also, as an integral part of EU policy, to promote trade liberalization and ensure that a single integrated market was achieved.' Levin and Nicholson, *supra* note 51, at 376, The EU Directive mentions economic and social progress, trade expansion (Recital 2, 56), and free flow of personal data (Art 1 (2) alongside the right to privacy (Recital 2, 9-11, 68 and Art 1(1). Specifically, see recital 3.

54 Gutwirth (2002: 91). For more on various issues relating to the human rights role of the EU, see Búrca(2011: 649-693).

55 Bernal (2011:268. The research also notes that 'so long as the primary focus remains on economic success, privacy and autonomy are likely to be squeezed'

56 Ibid.

57 UDHR, Article 12.

58 ICCPR, Article 17.

59 ECHR, Article 8. The African Charter on Human and Peoples' Rights (ACHPR), unfortunately, does not contain a right to privacy.

60 Kuner (2009: 308). Bygrave (2002:116).

61 For example US, Canada, Australia, New Zealand. In fact, Makulilo argues that 'that the two concepts are increasingly becoming synonymous and hence interchangeable in their daily uses.' Makulilo*w* (2012 166). See also Bygrave (2001: 277-283). Lloyd (2011: 26).

62 See for example the South African POPI Act, Preamble; See also EU Directive, Article 1. However, the Proposed EU Regulation however takes a different approach. It anchors data protection on the *sui generis* right to data protection. See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to The Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) COM(2012) 11 final 2012/0011 (COD), Article 1.

63 Bygrave (2002:122).

privacy, data protection seeks to protect other human rights and fundamental freedoms such as autonomy and human dignity.[64] Data protection law has over time become an area of concern for various core human rights institutions like the United Nations[65] and the Council of Europe (CoE).[66] DPAs also view data protection as a human right of universal application.[67] For example, the International Conference of Data Protection and Privacy Commissioners in one of its resolutions made at Strasbourg stated that 'the right to data protection and privacy are fundamental rights of every individual irrespective of his nationality or residence.'[68]

Based on the above, data protection can be said to be a composite human right because of its strong attachment to the right to privacy and other human rights. Some jurisdiction and scholars seem to have however extended this argument because of the immense contemporary significance of data protection.

C. The Emerging Position: The Right to Data Protection as an Autonomous Human Right

Rather than perceive data protection as a composite human right, there is an emerging movement comprising scholars and states that seem to bifurcate data protection and privacy. Starting from the EU legal order, data protection is now viewed as an independent human right. The EU Charter has separated data protection from the right to privacy.[69] The reason for this, as contended by De Hert and Gutwirth, is so as to substantiate the human rights basis of data protection which was hitherto heavily contested.[70] A number of countries in Europe also have separate provision on the right to data protection in the Bill of Rights of their Constitutions.[71] In the same vein, some authors have argued that the 'added value' of a right to data protection

---

64 Van der Sloot (2015: 26).

65 The preamble to the UN Charter states that the peoples of the UN are determined to, among others, 'reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small'. Charter of the United Nations, http://www.un.org/en/documents/charter/preamble.shtml accessed 23 February 2015. Apart from UN Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989), there are still calls for an international privacy and data protection framework under the umbrella of the UN. This was from the Monteux Declaration in which there was an appeal to the UN 'to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights.' De Terwange (2009:174-175). See also Kuner (2009: 308).

66 The council is Europe's leading human rights organisation. Council of Europe, 'The Council of Europe in Brief', http://www.coe.int/en/web/about-us/who-we-are accessed 23 February 2015.

67 De Terwange (2009: 174-175); Kuner (2009: 308).

68 See 30th International Conference of Data Protection and Privacy Commissioners. The protection of personal data and privacy in a globalized world: a universal right respecting diversities, Strasbourg (October 2008). https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/08-10-17_Strasbourg_international_standards_EN.pdf accessed 23 February 2015.

69 See Articles 7 and 8 of Charter of Fundamental Rights of the European Union, (2000/C 364/01), http://www.europarl.europa.eu/charter/pdf/text_en.pdf accessed 1 November 2014.

70 De Hert and Gutwirth (2009: 8).

71 Example, Belgian Constitution (1831), Article 22; Portuguese Constitution (1976), Article 26; Spanish Constitution (1978); Article 18 and Swedish Constitution (1975), Article 2. In other countries like Canada, data protection is a quasi-constitutional right. See the decision of the Canadian Supreme Court in *H.J. Heinz and Co. Ltd v. Canada (Attorney General)*, [2006] SCC 13, para. 28.

makes it distinct from the right to privacy and as such, must stand independently.[72] As an independent human right therefore, realisation of data protection must be within the context of the general principles of human rights.

D. Data Protection and the Principles of Human Rights

The gradual recognition of data protection as an independent human right has certain implications one of which is that it places an obligation on states to ensure the adequate protection of individuals' personal data. As with other human rights, certain principles must underpin data protection and govern its operation.[73] First, data protection is deemed to have an equal status with other human rights based on the principle of indivisibility of human rights.[74] Though of relatively recent origin, it is in no way of a lower status to other human rights. Besides, the right to protection of personal data is interrelated and dependent to a larger extent on other human rights like privacy, access to information,[75] dignity and autonomy. Hence, the fulfilment of the right to data protection depends, to a larger extent, on the fulfilment of these other rights. There is also an obligation on the state not to discriminate against individuals in the realisation of this right, thus, the digital divide[76] argument plays little or no role in this regard. This is so because data protection, as a human right, is deemed to be universally applicable to all persons irrespective of their status or class in the society.[77] States are therefore not only accountable for respecting and protecting the data protection, but must take positive action to facilitate its enjoyment.[78] This action may be in form of enacting relevant legislation or undertaking appropriate legal reforms.

The Legal Framework for the Protection of Personal data in Nigeria

There is presently no omnibus legislation on personal data protection in Nigeria. However, the right to personal data protection can be impliedly read in certain provisions of the Constitution, the common law and other statutory instruments.

A. The Constitution and the Common Law

The Constitution of Federal Republic of Nigeria (the Constitution) provides for the right to privacy.[79] Section 37 states that the '[t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.'[80]

---

72 Lynskey (2014).

73 Like the principles of human rights generally. Smith (2007: 29).

74 Based on the principles of international human rights outlined in United Nations Human Rights, 'What are human rights', http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx accessed 23 February 2015.

75 Although, it is acknowledged that the right to data protection and access to information are also in great tension. For more on this issue, see Banisar (2011).

76 Digital divide is 'the gap between those in society who have access to the Internet (broadband, in their homes) and those who have either poor access (dial-up connection at a public library) or no access at all.' See Stefanick (2011: 18).

77 Article 1 of the Universal Declaration of Human Rights 1948. 'All human beings are born free and equal in dignity and rights."

78 Ibid.

79 Constitution of the Federal Republic of Nigeria (1999).

80 Ibid, section 37.

Though the meaning of privacy within the context of this provision is not stated in the Constitution,[81] commentators have argued that the provision could be interpreted to also apply to personal data protection as narrowly construed.[82] This is because the express reference to citizens' correspondence, telephone conversations and telegraphic communications shows an intention to protect information privacy.[83] Notwithstanding that, the constitutional provision is limited in two ways for the purpose of data protection. First, even if it is argued that the provision may be broadly interpreted to include information privacy, information privacy is arguably only an aspect of data protection which guarantees the inaccessibility of private information.[84] Data protection is more of an open concept that is broad enough to cover opacity and transparency of personal data.[85] The second limitation is that personal data within the context of data protection must not necessarily be secret or confidential.[86] Personal information such as a person's name and address may not necessarily be private or secret, but will be personal data within the scheme of data protection law.[87] The greatest limitation of section 37 in protecting both privacy and data protection is that it applies only to citizens of Nigeria, thus it is debatably discriminatory.[88] Indeed, we have argued in the previous section that there should not be discrimination in the application of human rights.

Some authors also contend that the common law applicable in Nigeria also provides limited protection for personal data even though it does not recognise an independent tort of privacy.[89] It has been argued that an action for breach of confidence under the common law could apply to personal data protection to a certain degree.[90] However, an action for breach of confidence will be limited for personal data protection because breach of confidentiality anticipates a relationship of trust between the parties.[91] This may not, however, be the case with violation of the right to data protection. Furthermore, Laosebikan contends that the torts of trespass, defamation and nuisance are also applicable for the protection of personal information.[92] Like the Constitution, the common law protects only private and confidential information and not necessarily personal data as narrowly construed. Similarly, the common law does not anticipate the complexities of computerised processing of personal data that exists today.

B. Other Laws and Sectoral laws

A number of other laws provide sketchy protection for personal data in Nigeria. The Freedom of Information Act (FOI Act)[93] which grants the right of access to public records has certain

81 There are extremely limited court decisions on the right to privacy generally in Nigeria.
82 Nwauche (2007: 84). Allotey (2014: 173).
83 Ibid.
84 Schartum (2008).
85 Ibid. See also De Hert and Gutwirth (2006:61-104).
86 Schartum (2008); Abdulrauf (2014).
87 Ibid.
88 This is evident from the opening words of the section '[t]he privacy of citizens..'. Kusamotu (2007: 154). See also Dada (2012: 42).
89 Unlike some other jurisdictions that have an independent civil law of privacy like South Africa, Germany and some provinces in Canada.
90 Nwauche (2007:79). See also Laosebikan (2007: 340).
91 Solove (2007: 770).
92 Laosebikan (2007: 340-344).
93 Freedom of Information Act (2011).

provision that could be construed as being in tandem with the purpose of data protection law. Section 14 of the FOI Act, for example, provides that a public institution must deny an application for information that contains personal information.[94] It is, however, unclear if a person can be granted access to his/her own personal information in a public record based on this section. This would have made the FOI Act in line with the active control agenda of data protection law[95] which also has the effect of reducing power asymmetries between individuals and the government.[96] Section 14(2) of the FOI Act may arguably be relied upon by an individual to gain access to his/her personal data as it provides that a public institution shall disclose any information that contains personal information if the individuals to whom it relates consents to disclosure. This situation may therefore be as good as arguing that an individual has consented to the disclosure of his/her personal data in a public record.

The health sector is a sector in Nigeria which holds volumes of individuals' sensitive personal health information. Recently, the Nigerian National Health Act 2014 (Health Act) was enacted.[97] It contains very sketchy provisions on data protection. The Health Act places an obligation on the safety of health record on the person in charge of every health establishment.[98] It also provides that all information on a user's health status and treatment is confidential.[99] Personal health information may only be disclosed under certain circumstances which include consent, a court order and if non-disclosure represents a serious threat to public health.[100] There are penalties for failure to comply with the provisions of the law.[101] Another important sectoral law which has provisions on data protection is the Statistics Act of 2007.[102] However, like all the other laws discussed above, it protects the confidentiality of information.[103] Because of the current attention data protection attracts at various levels, one will assume that policy makers will seize the opportunity to introduce data protection principles in these relatively recent laws. Unfortunately, personal data protection was not considered as an issue deserving such attention.

The forgoing shows the limitation of the extant legal framework on personal data protection in Nigeria. Unfortunately, there are also no decided court cases in this regard. All these show that more needs to be done to protect Nigerians personal data in this computer age. The next part considers efforts made in this regard.

---

94 The provision further gives examples of information which is inaccessible to the public because it constitutes personal data.

95 For more on active control, see Neethling (2012: 245).

96 Lynskey (2014: 592).

97 Nigerian National Health Act (2014). Available at http://www.unicef.org/nigeria/ng_publications_national_health_bill_2008.pdf accessed on 20 January 2014.

98 Ibid, section 25.

99 Ibid, section 26 (1).

100 Ibid, section 26 (2).

101 Ibid, section 29.

102 Statistics Act (2007).

103 Ibid, section 26.

Attempts to Develop a Legal Framework on Personal Data Protection in Nigeria: An Analysis of Challenges to Legal Reforms

Arguably, the inclusion of the right to privacy in the Constitution imposes an obligation on the legislature to enact a law to protect privacy of personal data.[104] Therefore, several opportunities have come before policy makers to develop a quality legal framework that meets the challenges of personal data processing in Nigeria. These opportunities came up when considering draft legislative policies. This section considers these opportunities with a view to determining if they have been sufficiently utilised by Nigerian policy makers.

Though several attempts have been made to enact a legislation on data protection, not all the resulting draft bills focus specifically on data protection.[105] In this part, we consider only the bills that focus on data protection as narrowly construed earlier in this paper. This is because the *sui generis* right to data protection is more often than not protected via a specific legislation containing the FIPPs.

A. Critiquing of the Draft Bills on Data Protection in Nigeria

There are currently four draft bills supposedly on data protection in Nigeria. These are the Cyber Security and Data Protection Agency Bill,[106] the Privacy Bill;[107] the Data Protection Bill[108] and the Personal Information and Data Protection Bill.[109] It must be pointed out that none of these bills has been adopted.[110]

---

104 This is the view of Roos with regard the South African Constitution provision on Privacy. See Roos (2008: 354).

105 See for example the Computer Security and Critical Information Infrastructure Protection Bill (2005); Cyber Security and Data Protection Agency Bill 2008; Electronic Fraud Prohibition Bill 2008. In 2009, there was the Computer Security and Protection Agency Bill and Computer Misuse Bill. Then the Economic and Financial Crimes Commission Act (Amendment) Bill 2010 and the Cyber Security and Information Protection Agency Bill 2012. These entire draft bills have provisions related to data protection. They are all contained in the Nigerian National Assembly website at http://www.nassnig.org.

106 Available at http://www.nassnig.org/nass2/legislation.php?id=410 accessed 20 January 2015.

107 Available at http://www.nassnig.org/nass2/legislation2.php?search=privacy&Submit=Search accessed 20 January 2015.

108 http://www.nassnig.org/nass2/legislation2.php?search=data+protection&Submit=Search accessed 20 January 2015.

109 Personal Information and Data Protection Bill (2012), [Unfortunately, the Bill is not available online however, a copy is available on file with the authors].

110 T. Kio-Lawson, 'Right to be Forgotten', *Business Day* 1 June 2014 http://businessdayonline.com/2014/06/right-to-be-forgotten/#.VF5UKjTF9yJ accessed 20 January 2015.

The Cyber Security and Data Protection Agency (Establishment, etc.) Bill, 2008 has quite a number of provisions on cyber security. The objective of the Bill however is to establish a cyber security and information protection agency that is charged with the responsibility to secure computer systems and networks and liaise with relevant law enforcement agency for the enforcement of cybercrimes laws and related matters.[111] A close look at the Bill shows that it does not contain any provisions on the protection of personal information. The function of the proposed agency is strictly to combat cybercrime.[112] Even its definition of data shows that it does not anticipate personal data as narrowly construed by data protection laws.[113] We therefore submit that there is a contradiction between the title of the Bill and its contents. In fact, the title is misleading as one would expect that the Bill should establish a DPA responsible for enforcing data protection provisions. In any case, there is yet to be a substantive data protection legislation which therefore makes it surprising to see a bill establishing only an agency on data protection.

A second opportunity to enact a law on data protection came shortly thereafter in 2009 with the Privacy Bill.[114] Arguably, the Bill also envisages processing of personal data as narrowly construed by data protection law, even though it does not make use of the term 'data protection' or 'data privacy'. Section 1 of the Bill limits its scope to only government agencies. A critical examination of the Bill shows that its emphasis is on access to information rather than data protection.[115] The FIPPs which is the crux of data protection law are not explicitly provided for in the Bill even though some aspects of this can be read from its body.[116] This significantly makes its data protection agenda very suspicious as every data protection instrument should at least explicitly provide basic rules on data processing. The Bill also grants the government significant powers and exemptions for personal data processing.[117] It must be pointed out that the Bill contains provisions establishing a supervisory agency unlike the Data Protection Bill.[118] However, the requirement of independence for the data protection authority is absent in the Bill.[119] Section 48 which provides for the establishment of the Privacy Directorate requires that the directorate is established in the office of the federal ministry of justice which is an integral part of the executive arm of government. One therefore questions how the privacy directorate which is an integral part of the executive can sanction it (the executive) for illegal or wrongful personal data processing activities. It is our view that the Bill is merely a replication of the data protection law of other jurisdictions without proper in-depth study.[120] Finally, the Bill contains lots of inconsistencies and ambiguous provisions.[121]

---

111 Personal Information and Data Protection Bill (2012), Section 1.

112 Ibid. See the provisions of section 4 which contains the major functions of the agency.

113 Data is defined in section 38 of the Bill as 'a representation of information, knowledge, facts, concepts or instructions intended to be processed, being processed or has been processed in a network.' The Bill does not however contain a definition of 'processing'.

114 Privacy Bill 2009.

115 Ibid, see Part V.

116 Ibid, see for example processing limitation (sections 2 & 5); purpose specification (section 3); accuracy of personal information (section 4); consent (section 6).

117 Ibid, part IV & VI.

118 Ibid, part IX.

119 Ibid.

120 For example, the Privacy Act of Canada (1982) and the Privacy Act of the United States (1974).

121 A very clear example is the Section 2 which provides that '[n]o personal information shall be collected by a government institution unless it relates directly to an operating programme or activity of the institution.' The section does not say what is the meaning of 'an operating programme or activity' neither is it contained in the interpretation section (sec. 69). The Bill also distinguishes between various stages of processing of personal

The Data Protection Bill[122] is yet another opportunity by the Legislature to change the future of personal data protection in Nigeria. This Bill was presented to the Legislative House in 2010.[123] The objective of the Bill is to 'provide for personal data protection to regulate the processing of information and for related matters.'[124] This objective is however couched in a rather ambiguous and confusing language making it seem as if the objective of data protection is to regulate the processing of personal data when the opposite ought to be the case. Regulation of data processing is supposed to be for the purpose of protecting personal data.[125] The scope of application of the Bill is not indicated.[126] With respect to the principles of data protection which is the core of data protection law, the Bill's provisions are extremely vague and ambiguous.[127] However, some of the principles can only be implied from other provisions in the Bill such as the processing limitation and purpose specification principles;[128] the information quality principle[129] and the safeguard principle.[130] The Bill also contains certain rights of the data subjects. It provides that personal data shall be 'processed in accordance with the rights of the data subjects.'[131] Such rights include rights of access to personal data,[132] right to prevent processing likely to cause damage or distress,[133] right to prevent processing for purposes of direct marketing, [134] rights in relation to automated decision taking[135] and rights to rectification, blocking, erasure and destruction.[136]

Apart from the vague and incoherent nature of the Bill, a major weakness is that it does not provide for a dedicated supervisory agency.[137] The responsibility for supervising the implementation of the Bill seems to be on the courts.[138] This is particularly problematic as courts in Nigeria are generally known to be overloaded with cases which diminishes their effectiveness.[139] Moreover, data protection usually raises technical issues which require an independent specialised agency with the requisite technical expertise. Another problem with the draft Bill is its enforcement regime. The Bill does not contain serious penalties for violations of its provisions and it merely creates offences without stipulating punishments.[140] This runs afoul

---

data (i.e. collection, use and disclosure) which make its provisions very clumsy. Unfortunately, clarifications cannot be made as the Bill does not include an elaborate explanatory memorandum.

122 The Data Protection Bill (2010)..

123 See Greenleaf (2013).

124 Data Protection Bill, title.

125 Ibid, the explanatory memorandum seems more apt in this regard. It is stated that 'this Bill seeks to make provision for the regulation of the processing of information relating to individuals'.

126 Makulilo (2012: 26).

127 The principles are not expressly set out in the Bill, rather, sketchy provisions of some of them are contained in some sections of the law. See for example processing limitation (sections 2 & 5); purpose specification (section 3); accuracy of personal information (section 4); consent (section 6).

128 Data Protection Bill (2010), Sections 1(1)(a) and (b).

129 Ibid, section 1(1)(d).

130 Ibid, section 1 (3).

131 Ibid, section 1 (1)(e).

132 Ibid, section 2.

133 Ibid, section 3.

134 Ibid, section 4.

135 Ibid, section 5.

136 Ibid, section 7.

137 Makulilo (2012:26).

138 See for example sections 2(10); 4(2); 5 (5); 7 (1); 8(2)& (3); 9(3)(a).

139 A recent survey conducted in some states in Nigeria showed that over 60 percent of court users complained of excessive length of court proceedings. See NIALS (2000:19-21). See also Akanbi, (2012: 327).

140 See for example sections 8(3); (4); (5).

of the Constitution.[141] This is unfortunate because a law of this nature which purports to establish novel rights must be drafted in a very clear manner and must be in accordance with international prescripts on data protection. The Data Protection Bill in its present form presents a weak standard of data protection and may not sufficiently protect individuals if it is eventually enacted as law.[142]

The Personal Information and Data Protection Bill[143] is the most recent opportunity for legal reforms by policy makers. This Bill was proposed by the National Identity Management Commission (NIMC)[144] as part of its initiatives on data protection in Nigeria.[145] At a stakeholder workshop organised by the NIMC on the draft Bill, the then Minister of Justice and Attorney-General of the Federation commended this Bill as a long overdue initiative.[146] We must however point out that there is no evidence suggesting the Bill is before the Legislative House of Assembly.[147] The Bill has two broad objectives: it seeks to establish rules on the processing of personal information 'in a manner that recognises the right to privacy of individuals with respect to their personal information' and the need for organisations to process personal data for purposes that a *reasonable person will consider appropriate*.[148] The introduction of the requirement of reasonableness in the objective is problematic as it gives businesses a wide latitude to process information without recourse to the provisions of the Bill. The Bill applies to every person and organisation that collects, uses or discloses personal data in the course of commercial activities.[149] It has been criticised for the exclusion of government institutions from its scope.[150] This is surprising because the NIMC that proposed the Bill is a government entity that engages in mass processing of personal data. It therefore implies that the NIMC is sponsoring a bill and excluding itself from its scope. This is a contradiction.

Like the style adopted in data protection legislation in some jurisdictions such as Canada, the body of the Bill does not contain the FIPPs.[151] However, it is provided in section 3 that 'every organization shall comply with obligations set out in schedule 1.' Schedule 1 contains 'privacy principles for protection of personal information.' The exclusion of the principles from

---

141 Section 36 (12) of the Nigerian Constitution provides that 'Subject as otherwise provided by this Constitution, a person shall not be convicted of a criminal offence unless that offence is defined and the penalty therefor is prescribed in a written law, and in this subsection, a written law refers to an Act of the National Assembly or a Law of a State, any subsidiary legislation or instrument under the provisions of a law.' See and the case of *Aoko v. Fabgemi* (1963) 7 EN. L.R.1.

142 Makulilo (2012: 27).

143 Personal Information and Data Protection Bill.

144 The NIMC is an agency of the government with 'the mandate to establish, own, operate, maintain and manage the National Identity Database in Nigeria'. It is also to register persons within the scope of the Act and assign Unique National Identification Number (NIN). The NIMC also is to issue National Identity Cards to Nigerians. See https://www.nimc.gov.ng/ accessed 23 February 2015.

145 C. Idoko, 'Identity theft: FG proposes law on personal information, data protection' Nigerian Tribune Newspaper 22 February 2013 http://tribune.com.ng/news2013/index.php/en/component/k2/item/5812-identity-theft-fg-proposes-law-on-personal-information-date-protection accessed 20 January 2015.

146 "Nigeria: Adoke Lauds NIMC Proposed Draft Bill on Information, Data Protection" http://allafrica.com/stories/201302220301.html accessed 30 October 2016.

147 The Bill is not available in the National Assembly website online. See http://www.nassnig.org/ accessed 23 February 2015.

148 [Emphasis added].Personal Information and Data Protection Bill, Section 1.

149 Ibid, section 2(1)(a).

150 Ibid, Section 2(2)(a) and (b); See criticisms by Article 19 (2012:8).

151 The FIPPS are contained in the schedule of the Canadian PIPEDA. Available at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-3 accessed on 23 February 2014.

the body of the law makes it quite cumbersome because of the need for back and forth reading. This is a glaring weakness of the Bill.[152]

The Bill establishes the Office of the Privacy Commissioner who 'shall be responsible for implementation and administration of the Act.'[153] However, it does not provide for independence of the Privacy Commissioner as suggested in international data privacy codes.[154] Besides, the powers of the Privacy Commissioner are significantly watered down as he/she can only make recommendations and individuals whose rights have been violated must seek redress in the Federal High Court.[155] The Bill does not restrict transborder flow of personal data which seriously jeopardises security of personal data.[156] It is submitted that, in the event the Bill makes it to the Legislative House of Assembly, its ability to influence the desired level of data protection will be limited.

B. Analysing the Challenges to Legal Reforms on Data Protection in Nigeria

There are a number of explanations for the weak standard of the draft bills (and the overall data protection framework) and the failure of Nigerian policy makers to enact any of them as law. These explanations can be said to also be the general impediments to realisation of adequate data protection in Nigeria.

The first explanation for the poor state of data protection in Nigeria is sheer lack of commitment by the Nigerian government and the absence of political will. Policy makers in Nigeria do not view data protection as a priority issue which must be addressed. They seem to neglect (or are oblivious of) the human rights foundation of data protection. Perhaps Nigeria's poor human rights track record[157] has a role to play in this lackadaisical attitude of the government. Unlike cybercrime that has attracted relatively more attention from the government recently, data protection is an area that is totally neglected.[158] The neglect is further depicted by the fact that it is almost 10 years since the first bill in this area surfaced and none is yet to be passed as law by the parliament. Meanwhile, laws of equal contemporary relevance, like the FOI Act and the Electronic Communications and Transactions Act, have since been enacted. Laws in Nigeria also do not keep pace with rapid advances in IT.[159] The government is rather reactive than proactive in dealing with the challenges brought about by IT. For example, it was not until cybercrime became such an international embarrassment before the Nigerian government gave it the attention it deserves.[160] Lack of commitment by the government is also depicted by the poor implementation of the available weak regulations on data protection. Unfortunately, the Nigeria courts too have made little or no impact on privacy issues generally.

---

152 Article 19 (2012: 6).

153 Personal Information and Data Protection Bill, section 4.1(7).

154 For example, UN Guidelines for the Regulation of Computerized Personal Data Files, Article 8; EU Directive, Article 28; AU Convention on Cyber Security and Personal Data Protection, Article 11(1).

155 Personal Information and Data Protection Bill, section 8 (3)(b).

156 For example, section 72 of the POPI Act of South Africa restricts transborder flow of personal information subject to certain exceptions contained in subsection 1(a-e) of the section.

157 Akinrinade (2002: 125).

158 See generally Abdulrauf (2014).

159 This fact has been admitted by even the Nigerian Attorney General to the Federation and Minister of Justice. See C. Idoko, 'Identity theft: FG proposes law on personal information, data protection' Nigerian Tribune Newspaper 22 February 2013 http://tribune.com.ng/news2013/index.php/en/component/k2/item/5812-identity-theft-fg-proposes-law-on-personal-information-date-protection accessed 20 January 2015.

160 See generally Ani (n.d: 197-323).

Another fact that emerges from the brief analysis of the various draft bills is that policy makers lack the basic understanding of the importance and rudiments of data protection. Two discernible points in the examination of the bills justify view. The first is that the bills exhibit a case of 'cut and paste' like many African countries do.[161] They contain many inconsistent provisions and weak data protection standards. Second, these draft bills lack expert touch. Rather than consult experts in data protection law, ordinary lawyers are contracted to draft the bills.[162] In spite of the rapid advances in ICT in Nigeria, the technical knowledge needed to design legislative frameworks to keep pace with these developments remains in short supply.[163] Shaping and implementing data protection policies are quite complex activities which require expertise and time.[164] There are insufficient debates, discussions and public consultations as many countries do for a technical bill on a subject like data protection. In South Africa for example, the data protection law, POPI Act, is said to be one of the "longest serving bills before the parliament."[165] The lengthy and robust deliberations gave the drafters opportunity to draw key lessons from other jurisdictions and consult widely. Besides, experts in the field constituted a research group which produced a 860 paged in-depth discussion paper/report.[166] In Nigeria on the other hand, there is no evidence suggesting any detailed research or discussion on any of the draft bill. In fact, there is virtually no official reports, media reports and statement by officials on data protection.[167] All these goes to show the level of commitment toward the subject matter.

A third challenge to data protection is the incoherence and the multiplicity of policies in the area. The Privacy Bill, Data Protection Bill and Protection of Personal Information Bill virtually have the same objectives, albeit with different scopes. Questions arise as to why there is a need to have various draft bills without passing any as law. An explanation for this is that politicians merely seek to attract the attention and publicity that comes with sponsoring a bill before the legislative assembly. This will send a message to their constituencies that they performing legislators. Hence, they do not care if there is already in existence a pending legislation. Besides, law making process in Nigeria is now deeply commercialised and compromised.[168] Obviously, a subject matter like data protection will attract little or no pecuniary benefit to legislators.

---

161 Makulilo (2013: 50).

162 Generally, lawyers assist legislators in drafting of bills in Nigeria. This is because most legislators do not have a legal background. In fact, there is a legal drafting department in the legislative house comprising just lawyers. See "Legislative Law Practice is an Evolving Area of Legal Practice in Nigeria"http://www.thisdaylive.com/index.php/2016/06/14/legislative-law-practice-is-an-evolving-area-of-legal-practice-in-nigeria/ accessed 30 October 2016 The argument we are trying to make with regard to data protection is that most of these lawyers do not possess the requisite technical knowledge on the nitty-gritties of data protection.

163 Gwagwa notes this in relation to Africa generally. A. Gwaga et al 'Protecting the right to privacy in Africa in the digital age', http://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf accessed 20 January 2015.

164 Flaherty (2007).

165 P Stein 'South Africa's EU-style data protection law' (2012) 10 Without Prejudice 48 also available at http://reference.sabinet.co.za/document/EJC128763 (accessed 1 November 2015).

166 South African Law Reform Commission (SALRC) "Privacy and Data Protection" (2009) http://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf accessed 30 October 2016.

167 An extensive search of the internet will justify this point. This is unlike South Africa where official documents on the deliberations prior to the law are widely available on the internet.

168 "Challenges Of Legislative Intellectualism Before The Eight National Assembly Of Nigeria" https://www.thenigerianvoice.com/sports/179835/challenges-of-legislative-intellectualism-before-the-eight-national-assembly-of-nigeria.html accessed 30 October 2016/

Likewise, various sectoral regulations that have to do with data protection in Nigeria are incoherent and conflicting. This also goes to show the lack of appreciation of the rudiments of data protection by policy makers.

A fourth challenge to legal reforms on data protection in Nigeria is low level of awareness. In a recent study of the attitude of Nigerians towards data protection however, the investigators found that quite a number of the respondents were actually aware of some of the risks but are simply not bothered.[169] Notwithstanding this, it is our view that the average citizen is not aware of the gamut of risks involved in the proliferation of his/her personal information in the cyberspace *sans* regulations.[170] In this regard, Bakibinga observes that Africans generally suffer from 'privacy myopia' which means they underestimate the value of their personal data and the need for its protection.[171] With such low level of awareness, the people cannot be engaged for quality discussions and consultation on data protection issues. Obviously, no meaningful contribution will come out of such engagement. Similarly, the lack of judicial activism on data protection by the courts can be said to be because the people do not approach the courts challenging violation of personal data. This also borders on the level of awareness.

Security challenge is a fifth reason for the poor state of data protection legal framework in Nigeria. The Government is always weary of policies that restrict surveillance activities both online and offline under the guise of public safety and national security. They are also suspicious of any legislation that has the effect of enhancing access to information and the individuals' right to control the use of their personal data. The Personal Information and Data Protection Bill as we have seen earlier does not apply to government agencies.

In spite of all the above, the issue of concern to legal academics and human rights activist is what are the prospects for legal reforms in Nigeria given its peculiar nature.

Prospects and Options for Policy Makers and Stakeholders towards Legal reforms

The forgoing shows that the present state of affairs with respect to data protection in Nigeria leaves much to be desired. Unfortunately, policy makers do not seem to appreciate the risks posed by the absence of a legal framework on data protection. The prospects for the future will depend on greater commitment by the policy makers towards changing the *status quo.* Nigeria's delays in responding to the challenges of personal data proliferation may be converted to an advantage as it will create an opportunity for it to draw appropriate lessons from other jurisdictions since data protection laws has tremendously proliferated in the last few years, especially in Africa. In more practical terms, certain measures can be taken for a more effective regime on personal data protection in Nigeria.

First, there is the need to recognise data protection as a human rights issue that must be given priority. It is usually said that the first step towards addressing a problem is recognising it and acknowledging it as a problem. Better knowledge by relevant stakeholders of the dangers of personal data processing without an appropriate legal framework is vital for a future policy on data protection to work effectively. The government, data controllers/users and the people must have a moderate level of understanding on data protection issues. The level of awareness of the people is particularly crucial in this respect as it has been rightly opined that 'the more we know,

169 See generally Dawson et al (2015: 113-124).
170 Jemilohun (2010: 116).
171 Bakibinga (2004).

the more we seem to care, and ultimately companies and governments have to take account of that.'[172] Obviously, many Nigerians will readily object if they are aware of the gamut of risks involved in uncontrolled dissemination of their personal information. There is therefore a need to recognise that data protection raises issues beyond the traditional idea of right to private and family life.[173]

To enhance the level of awareness and understanding of data protection issues, the role of a DPA is paramount.[174] However, in the absence of a DPA in Nigeria, the National Human Rights Commission (NHRC) should take up this role as a starting point. The NHRC is particularly suited for this task because of its statutory mandate and regional obligation under Article 26 of the African Charter on Human and Peoples' Rights (ACHPR) of engaging in human rights education.[175] Its extended mandate 'to include vetting of legislation at all levels to ensure their compliance with human rights norms'[176] also make their role crucial in this regard. Moreover, scholars recommend future interactions between DPA and national human rights institutions as essential for more effective personal data protection at national levels.[177]

The role of human rights activists, public defenders and Non-Governmental Organisations (NGOs) is indispensable in enlightening people on various privacy and data protection issues. There are quite a number of NGOs who are making efforts towards sensitisation of the people on their privacy rights in the digital age.[178] These entities have made efforts especially with their country-based publications on privacy and data protection issues and other activities.[179] For example, the Data and Knowledge Information Privacy Protection Initiative (DKIPP), in commemoration of this year's Data Privacy Day, organised a workshop to sensitise participants on "the growing problem of data privacy vulnerabilities."[180] This is a welcome initiative which should be encouraged at a wide scale.

Second, there is the need for an 'appropriate' legal framework for personal data protection in Nigeria. Appropriate in this regard should not be a mere 'cut and paste' or transplant of data protection laws of other jurisdictions like most African Countries do[181] and as recommended by some academics.[182] An appropriate legal framework must consider all existing and future data protection issues in the Nigerian context and should be made to appeal to all the relevant stakeholders. The relevant members of the legislative house committee on privacy and human rights issues must possess some basic knowledge of data protection so as to promote legal

---

172 Bernal (2014: xii). See also Adelola et al (2014: 236).

173 Jemilohun (2010:116).

174 One of their paramount function includes education and awareness on data protection issues

175 See *Report on state of compliance with International Minimum Standards of Human Rights by Nigeria under the Universal Periodic Review Mechanism*, available at http://www.upr-info.org/sites/default/files/document/nigeria/session_17_-_october_2013/nhrc-nigeria_upr17_nga_e_main.pdfaccessed 23 February 2015. For the general mandate of the National Human Rights Commission in Nigeria, See Section 5 of the National Human Rights Commission Act 1995 nigeriarights.gov.ng/files/download/44 accessed on 23 February 2015.

176 NHRC 'Mandate' http://nigeriarights.gov.ng/mandate accessed 23 February 2015.

177 See Hustinx (2013: 157-172).

178 Examples of such NGOs include Art 19, EPIC and Privacy International. See *infra* note 192, 191 and 192.

179 For example, Article 19(2012:146); EPIC: Privacy and Human Rights Reports 2006, Federal Republic of Nigeria, available at http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Federal-3.html accessed 23 February 2015.

180 Bankole Orimisan "Experts warn Nigerians on abuse of data privacy" *The Guardian* 3 February 2016 http://guardian.ng/technology/experts-warn-nigerians-on-abuse-of-data-privacy/ accessed 1 November 2016.

181 Makulilo (2013: 50).

182 See for example Jemilohun (2010:116), See also Kusamotu (2007).

reforms.[183] Two other entities are critical for an appropriate legal framework. First, the Nigerian Law Reforms Commission (NLRC) must conduct sufficient research and consult with all relevant stakeholders.[184] Second, a committee of experts on the law of data protection should be constituted by Nigerian law makers to undertake the task of research and drafting of a proposed law. Drawing lessons from a jurisdiction like South Africa is instructive in this regard[185] as scholars have over time discussed the importance of lesson-drawing in data (privacy) protection policy formulations.[186] Lesson-drawing, it must be noted, does not only involve learning the positive features of a regime but also drawing lessons from the negative sides so as to avoid pitfalls. In considering an appropriate legal framework, two important issues must be considered based on the experiences of other jurisdictions. First, the proposed legislation must adopt a phased implementation strategy[187] because of the difficulty of implementing such sweeping legislation within a short period of time. Second, the law must contain a review mechanism as advances in technology and related issues are in a constant state of flux.

Because of the cross-border nature of data protection issues, Nigeria must seriously reconsider its commitments under regional and sub-regional instruments on data protection. The AU Convention on Cyber Security and Data Protection that is yet to be ratified must be ratified within the shortest possible time.[188] Although, this Convention has some lapses as elaborately discussed elsewhere,[189] it is at least a step in the right direction toward the realisation of the right to data protection. In addition, Nigeria must respect its obligations under the ECOWAS Supplementary Act on Data Protection which is already legally binding since it is an integral part of the ECOWAS Treaty.[190] The question of whether both regional instruments can prove effective, proportionate and compatible with competing rights is highly debatable. Nevertheless, since both regional instruments are largely inspired by the EU framework, they may arguably provide some initial guidance towards effective data protection. International agreements on data

---

183 See Flaherty's discussions with regard to the reform on the Canadian Privacy Act. Flaherty (n.d:30).

184 The NLRC is set up to "undertake the progressive development and reform of substantive and procedural law applicable in Nigeria by way of codification, elimination of anomalous or obsolete laws and general simplification of the law in accordance with general directions issued by the Government, from time to time and for matters connected therewith." See the Title of the NLRC Act, available at http://kyg.nigeriagovernance.org/Attachments/Organization/Act/67_Law_NIGERIAN%20LAW%20REFORM%20COMMISSION%20ACT.pdf accessed 23 February 2015.Section 5 contains the general functions of the NLRC. The project leading to the South African POPIA was carried out under the aegis of the South African Law Reform Commission (SALRC) and the project was entitled 'privacy and data protection'. See Van der Merwe (2014: 305).

185 The discussions on the Protection of Personal Information Act not only took a very long period of time, the project committee comprised of renowned experts in data protection and Information technology law such as Professors Johann Neethling & Ian Currie. The Committee was actually under the Chairmanship of Justice CT Howie however, Prof Neethling was the Project Leader. See SALRC "Privacy and Data Protection Report" (2009) available at http://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf accessed 23 February 2015.

186 See Bennett (1990: 551-570). In a related discussion, Bygrave talks about a cross-national perspective as being analytically fruitful for data protection as against comparative approach which itself may be important because all data protection regime are largely based on the same standards. See Bygrave (2002: 12); SALRC (2009:173, 615).

187 For Example, the PIPEDA of Canada adopted a phased implementation strategy over some period of time.

188 Details of the convention and its status list is yet to be uploaded on the AU website. http://www.au.int/en/treaties accessed 20 January 2015.

189 Abdulrauf and Fombad (2016).

190 See ECOWAS Supplementary Act, Article 48.

protection such as the Council of Europe's Convention may also be ratified by the government.[191] This will enhance transnational flow of ideas on data protection.

The third measure to be taken for the realisation of the right to personal data protection in Nigeria is that a dedicated institutional mechanism should be put in place for the purpose of oversight, implementation and enforcement of any new legislation adopted. The success of this measure is fully dependent on the previous points. When there is adequate comprehension of data protection issues and there is a quality legal framework on data protection, the problem of implementation and enforcement is largely taken care of. With respect to enforcement body, Nigeria has a range of options to adopt. Either the enforcement body should have far reaching powers[192] or adopt an ombudsman style.[193] But then, the supervisory body must be able to perform its functions independently.[194] The courts may also be strengthened to perform the role of enforcement and implementation. However, it must be noted that the role of a dedicated agency cannot be substituted with that of the court that lacks the requisite expertise on data protection issues. All is however dependent on the recommendations of the NLRC and the committee of experts after conducting extensive research and consultations.

Finally, there is the need to beef up the level of scholarship on data protection in Nigeria. Presently, there are very few scholars who focus their research solely on data protection.[195] More scholarship on data protection will enable Nigeria participate in various discussions and debates on personal data protection globally. This will also enhance expert network which is very crucial for the development of the jurisprudence on data protection.[196] Relevant stakeholders may also collaborate with bodies such as the Electronic Privacy Information Center (EPIC),[197] Privacy International[198] and International Association of Privacy Professionals (IAPP)[199] who have researched worldwide privacy policies. To further boost research output on data protection, integration between IT law and human rights law (and related issues such as data protection) should form part of the curriculum in universities both at the undergraduate and postgraduate levels. Presently, no institution in Nigeria teaches IT law as an undergraduate course.[200] At the

---

191 With the recent reforms being carried out in the Council of Europe's Convention in the name of 'modenisation' and 'globalisation', non-European countries could be ratify. Uruguay is in the process of ratifying. See generally Greenleaf (2013); Greenleaf (2013: 20-23).

192 Based on the European Model.

193 Based on the model adopted by Canada.

194 Greenleaf (2012:39).

195 That is with the exception of a few scholars (to the best of our knowledge) who have undertaken their doctoral researches on data protection like A.K.E Allotey and O. Laosebikan.

196 Makulilo (2012:178).

197 EPIC is an independent non-profit research centre that researches on issues of privacy, freedom of expression, democratic values, and promoting public voice in decisions concerning the future of the internet. It pursues a wide range of programmes including public education, litigation, and advocacy. EPIC is located in Washington, DC. Epic.org 'About EPIC' https://epic.org/epic/about.html accessed on 23 February 2015.

198 Privacy International is a London-based charity that investigated government surveillance activities and expose companies facilitating it. It engages in litigations, advocacy and research on issues of privacy, human rights and technology. Privacy International https://www.privacyinternational.org/ accessed 23 February 2015.

199 IAPP is an institution for training of professionals who want to advance their careers on data protection. https://www.privacyassociation.org/about accessed 23 February 2015.

200 Interaction with the Dean, Faculty of Law, University of Ilorin, Nigeria on 20 December 2014. He also stressed the fact that unfortunately, there seems to be no plan for any university to introduce IT law at the undergraduate level because of two main reasons. First, dearth of experts on IT law and second, IT law is not included in the accreditation requirement for law degree programmes by the National Universities Commission and Council of Legal Education in Nigeria.

postgraduate level, to the best of our knowledge, only one school teaches IT law.[201] Rather that jam-pack undergraduate curricula with studies on western legal system, IT law, with data protection prominent in the curriculum should be introduced at the degree levels in Nigerian institutions. But such should be done with a special focus on data protection issues arising in the African or Nigeria context.[202]

Conclusion

This paper situates the global debate on data protection in the Nigerian context. Discussions on this issue is crucial because of the strategic position the country occupies regionally and globally and in the wake of the country's gradual advances in technology. We therefore reflected on opportunities, options and challenges to legal reforms on data protection. In so-doing, we established the very critical place of data protection in the country by identifying a number of issues that directly threatens personal data and the individuals' subject of the data. We argued that the growing level of ICT penetration in the country has further strengthened its strategic place. Consequently, a brief analysis of the legal framework for data protection was carried out. We unpacked the nature and scope of data protection and considered its contemporary status as a human right. Contextualising data protection as a human right is necessary for two reasons. First, it buttresses the critical place of data protection in any country and second, it shows the responsibility of the government to ensure that an appropriate legal framework is established for its realisation. We contended that this fact has been acknowledged in some jurisdictions which is a reason why data protection occupies a strategic place as an independent right in the constitutions of these countries. Unfortunately, similar relevance has not been accorded to data protection in Nigeria.

An examination of the legal regime of data protection in Nigeria led to the conclusion that the extant framework cannot contain the increasing challenges to personal data. This is more so with the complexities of data protection issues in this computer age. An analysis of the draft bills on data protection showed that they may suffer similar fate of inadequate protection of personal data in the event any of them is enacted as law. This is because they contain weak standards and are lacking in some of the basic features of a modern data protection instrument. We identified reasons for the weaknesses of the draft bills and the overall legal framework on data protection and argued that such is largely due to lack of appreciation of the rudiments and value of data protection. From all the challenges discussed, we proffered our thoughts on certain legal and practical reforms necessary for enhancing adequate data protection in Nigeria. The prospects for the future are however largely dependent on greater commitment by policy makers.

Acknowledgements: We thank the two anonymous reviewers for their critical and insightful comments. All errors and omissions are ours.

[201] Presently, only University of Ilorin teaches IT law. The title of the course is Information and Technology Law, BUL659 & BUL 660 for 1st and 2nd semesters. They are however elective law courses.

[202] There is a movement in African academic circles on the need for Africanisation of legal education programmes in African institutions. See for example Fombad (2014:383-398).