Data protection in an emerging digital economy; the case of Nigerian Communications Commission: Regulation without predictability?

Aaron Olaniyi Salau*

Abstract

Since opening up the Nigerian telecommunications sub-sector to private mobile telecom providers in 2001 and until 2008, the industry regulatory body, the Nigerian Communications Commission (NCC) had no framework for registration of subscriber information. In 2011 the NCC issued a 'time-framed' Regulations for biometric data capture and personal information registration of existing and new subscribers though no data privacy or protection law exists in Nigeria. This paper argues that safeguards proposed in the NCC's Registration of Telephone Subscribers Regulations, 2011 ('NCC Regulations') concerning processing and storage of phone subscribers' personal information offers little protection to data, privacy and subscribers' other rights and falls below international standards. Part 1 of the paper gives background information on the regulatory context of an emerging digital economy in which the NCC operates. Part 2 undertakes an analysis of rationales for data protection internationally, especially in Europe. Part 3 problematises the underdeveloped right to data protection under the Nigerian Constitution vis-a-vis the 'NCC Regulations'. It discusses the effect of weak safeguards and remedies against misuse of subscriber information by service providers coupled with an untested right to data protection. Part 4 concludes and proposes safeguards against weaknesses existing in the law.

Keywords: Data protection, mobile phone, Nigerian Communications Commission, privacy, Nigeria

1. Introduction

Against the background of an astronomically rising telecommunications industry, this introductory section sets the scene for the rest of the paper. It catalogues the dividends of liberalisation of digital telecommunications, and outlines the basis of credible regulation of the telecommunications industry in Nigeria.

Africa's mobile telephony industry is witnessing tremendous growth, thanks to the wave of deregulation and privatisation of the telecommunications subsector that swept across the

continent since the early 1990s.[1] Nigeria joined this trend in 1992, and has become Africa's largest mobile telecommunications sector.[2] Full liberalisation took root in early 2000 through the formulation and implementation of the National Communications Policy 2000. Complete re-organisation and transformation of the sector came about with the enactment of the Nigeria Communications Act 2003[3] ('the NCA 2003') which made the Nigerian Communications Commission (NCC) the sole and independent regulator of the Communications industry. The Nigerian Telecommunications Act No. 75 of 1992, which established the Nigerian Communications Commission (NCC) was repealed while enunciation of National Communications policy 2000 together with the NCA 2003 opened up the sector to influx of foreign capital and local private investments.

Telecoms sector deregulation in Africa has generated rapid diffusion of mobile information and communication technologies (MICT) and spin-off services like online marketing and internet banking.[4] According to the international Telecommunications Union (ITU) forecast, Africa is expected to witness the strongest growth in mobile cellular phones by the end of 2014.[5] As at January 2016, Nigeria had a total of 151,357,769active subscribers divided into mobile (GSM) lines: 149,022,919; mobile (CDMA) lines: 2,147,982 and fixed wired/wireless lines: 186,868[6] (though the total figure for connected lines is not yet available due to the ongoing SIM card registration). As at December 2014, GSM lines accounted for 98.30% of total telephony market, the Mobile CDMA lines 9.36% while the Fixed Wired/Wireless segment had a paltry 0.14%.[7] The new lease of life brought to Nigerians by improving telecommunications infrastructure and expanding access to services testifies to the gains and market potentials unlocked by deregulation. The NCC has licenced a national carrier - Globacom Nigeria Limited (GLO) – and three other long distance GSM operators – MTN,

---

* PhD Candidate, Department of Public Law, Faculty of Law, University of Cape Town, South Africa.

[1] N Jentzsch Implications of mandatory registration of mobile phone users in Africa Telecommunications Policy (2012) 36 608–620 at 1.

[2] C B Opata Regulatory Accountability in the Nigerian Telecommunications Sector *JAL* (2013) 57 283–309.

[3] Act No. 19 of 2003 published in Federal Republic of Nigeria Official Gazette No. 62 Vol. 90 (Government Notice No. 115) of 19th August, 2003.

[4] J Aker & I Mbiti Mobile Phones and Economic Development in Africa **(**2010) 24 *Journal of Economic Perspectives* 207-32.

[5] See ITU "The World in 2014, ICT Facts and Figures", online:ICThttp://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf> (accessed 15 January 2016).

[6] NCC 'Subscriber Statistics' available at http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&Itemid=73 (accessed 28 March 2016).

[7] The Nigerian Telecommunications Commission *2014 Year End Subscriber/Network Data Report For Telecommunications Operating Companies in Nigeria* NCC Statistics-Annual_Industry_Statistics_Report_2014.pdf 1 (accessed 28 March 2016).

Airtel (formerly Econet) Nigeria Limited and MTS (Etisalat). Excepting GLO, the other three multinational companies. These companies and numerous others provide various telecoms, internet and ICT-related services. The unparalleled foreign investments in mobile telephone networks and telephone-related services has resulted into massive ownership and use of mobile handsets.[8] The availability of low-cost hand-sets coupled with affordable access tariffs have further enabled remotely located rural dwellers, the poor and low income earners to connect locally and internationally with far flung urban-based populations in real time.

Industry reform has brought multiplier effects not only on the telecommunications industry but the entire Nigerian economy in terms of overall investments, trades and services such that the telecoms subsector has been contributing an average of 8 percent per annum to Nigeria's overall Gross Domestic Product (GDP) since 2000.[9] A combination of market liberalisation, competition and economies of scale have led to a lowering of access costs and lifted barriers to mobile interconnectivity through introduction of innovative billing tariff plans. The ubiquitous nature of mobile telephony and the social services provided by production, advertisement, distribution and wholesale marketing of recharge cards, mobile hand-sets and vending of subscriber identification module (SIM) cards[10] for multiple mobile networks have created job opportunities for hitherto unemployed rural and urban poor. The value-added services associated with mobile telephony like internet connectivity provided by mobile phone companies and licenced internet service providers (ISPs) have created rapid expansion of internet services using Wi-Fi technologies.[11] Nigeria is also a budding market for 'smart phones' enabled for convergence of voice and data services. All of these make Nigeria's telecoms industry an emerging powerhouse in the African digitalised mobile telephone services.

This quantum leap did not come without some structural changes. It came about due to lenient national deregulation policies and the growing independent regulation of telecommunication services. The establishment of clear framework for independent regulation of the Nigerian telecommunications industry was in itself part of an adaptation to a

[8] Ibid. Facts and figures available in NCC publications and website depict similar multiplier effects of regulatory action taken in the industry from 2001 to 2015 on job employment opportunities, community development and other communication-related activities.
[9] Ibid.
[10] This is the card issued by mobile phone operators which provides the individual user with the appropriate number recognized by that network which a subscriber inserts into a mobile phone to access the mobile phone network. See 'SIM Registration' available at http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=122&Itemid=113
[11] ITU op cit n 5 19.

global policy shift from state-owned monopolies towards market competition in the last quarter of a century.[12]

According to the ITU, a basic prerequisite for credible and stable regulation of the telecommunications industry is the existence of clear legislative framework, capacity and professional ability of the industry regulator.[13] Indeed, Nigeria had been commended for adopting 'a clear policy for the development of the telecommunication sector, supported with a flexible regulatory framework' the major policy thrust of which was the economic regulation of the telecommunications sector.[14] The NCC was established as a semi-autonomous regulatory body within the ambit of overarching objectives of the National Telecommunication Policy 2000, which is 'national socio-economic development and seamless national integration into global communication networks in an efficient, affordable and reliable manner.[15] For the NCC therefore, as stated above, the legal and policy frameworks consist of the Telegraphy Act 1990,[16] the NCA 2003 and the National Telecommunications Policy 2000.[17] The NCC's regulatory mandate empowers it to engage in a great number of activities. These, among others, are to specify and publish technical codes and specifications;[18] prepare or require licensees or a designated industry body to prepare consumer codes;[19] determine, administer, monitor and enforce compliance with competition and anti-competition laws[20] on market domination[21] and interconnection[22] and ensure universal access for unserved, underserved areas and underserved groups.[23] Aside from technical conformity with the law, it can be argued that for consistency and predictability, these extensive rule-making powers, other functions of the Commission and objectives of the NCA 2003 must be exercised in the public interest and with regard for openness and consultations with stakeholders including the general public. The NCC has seized upon the

[12] C B Opata op cit n 2 at 283.
[13] Ibid at 9 and 21.
[14] Ibid at 3.
[15] Ibid at 12.
[16] No. 31 1998.
[17] The primary function of the NCC includes the promotion of investments and private sector participation; the facilitation of entry into the industry and healthy competition among operators; implementation of standards and monitoring of operators for efficient and qualitative service; expansion of the nation's communication facilities; ensuring universal access to affordable telecommunications service for all Nigerians; management of the Universal Access Fund and protection of consumers. See s 4*(a)-(w)* of the NCA 2003; the Telegraphy Act No. 31 of 1998 and the National Telecommunications Policy 2000.
[18] NCA 2003, s 130(1).
[19] NCA 2003, s 106(1)(2)(3)*(a)(b)(c)*(4)*(a)(b)(c)(d)(e)(f)*(5)(6).
[20] NCA 2003, ss and 91.
[21] NCA 2003, s 90.
[22] NCA 2003, ss 96 and 97.
[23] NCA 2003, s 112.

broad mandate of 'economic and technical regulation' of the industry granted by the NCA 2003[24] and other enabling Acts to establish innovative licences and prescribe conditions relating thereto. The NCC has crafted regulations on interconnectivity and consumer protection and lately, established subscriber information registration procedures to activate SIM cards.

However, the success story of digitised telecommunications in Africa is being marred by rising wave of mobile-phone related criminality culminating in the introduction of SIM card registration policies in most African countries[25] including Nigeria.[26] As in other many other African countries, the downside of Nigeria's telecoms industry successes is the ascription of rising wave of criminality to the widespread availability of unregistered SIM cards. According to interactions between security agencies and the NCC, the increasing difficulty of apprehending kidnappers who demand ransom from their victims' families through mobile phones, and resolving other phone-related crimes is fast becoming a security nightmare. This anonymity advantage of unregistered SIM cards seems to be attractive to criminals. Despite lack of data or research conclusively connecting availability of unregistered SIMs to increased kidnappings, the NCC seemed to have bowed to pressure to introduce a SIM card registration policy. The NCC Regulations which it introduced effective from 2011 provides for mandatory biometrics data capture and registration of personal information of mobile phone subscribers. But before probing further the utility of the Regulations, the next subsection delves into standards of protection afforded by international data protection laws.

2. Data Protection Rationale and Privacy Standards

Technological convergence, globalisation, diffusion of intrusive technologies and interconnectedness of national telecommunication networks have made data security more imperative. The risks to individual rights inherent in fast dissemination, automatic processing and transfer of information at unimaginable speeds by modern digital telecommunication services have always made them attractive for state regulation. Data protection laws therefore focus on data processing, which is the automated or manual collection, registration, storage,

[24] NCA 2003, s 2(1)*(w).*
[25] K P Donovan & A K Martin The rise of African SIM registration: The emerging dynamics of regulatory change *First Monday*, Volume 19, Number 2 - 3 February 2014 available at http://www.firstmonday.dk/ojs/index.php/fm/article/view/4351/3820
doi: http://dx.doi.org/10.5210/fm.v19i2.4351.
[26] See the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 S. I. No. 35 published in Government Notice No. 229 Federal Republic of Nigeria Official Gazette No. 101 of 7th November, 2011 Vol. 98 (hereinafter referred to as 'the NCC Regulations').

use or dissemination of personal information.[27] Personal data has also been defined as the information that can be used to identify a natural individual.[28] The information can relate to a person's personal details, gender, health status, personal relationships, telephone calls, internet activities, banking transactions, etc. As such, data protection laws provide legal cover to the individual against misuse, misappropriation or unlawful disclosure of her personal information. The right to privacy uphold values such as dignity, autonomy and personality, which also underlie data protection, hence, most privacy laws often harbour data protection principles.[29] However, a conceptual clarification between data protection and privacy is beneficial. This clarification better serves human dignity because, as it was rightly observed, 'the latter serves a multiplicity of interest beyond privacy concerns'.[30] Based on the understanding that the right to privacy is a pillar of data protection, the following sections respectively engage with the concept of privacy, and the ethical foundations for data protection under international law, European standards and African prescriptions. The overall aim is to determine what these regimes offer as safeguards against misuse of telephone subscribers' information.

2.1. Defining privacy

Definitions of privacy vary widely according to context and environment. Components of privacy are wide reaching and extend to ability to protect ones bodily integrity, physical zones of intimacy,[31] and informational about oneself.[32] The emphasis in this paper is given to informational privacy. This idea of privacy posits that certain spheres of intimate individual activities involving personal information are inviolable and protected from monitoring by the State or other individuals and through secret surveillance. For example, Mill posits that 'there is a circle around every individual human being, which no government… ought to be

[27] A Roos 'Data protection' in D Van der Merwe et al *Information and communications technology law* (2008) 313.
[28] L A Bygrave Data Protection Pursuant to the Right to Privacy in Human Rights Treaties International *Journal of Law and Information Technology* 6 249-268.
[29] A few examples from Australia are: the Privacy Amendment (Private Sector) Act 2000 (Cth); Privacy and Personal Information Protection Act 1998 (NSW); Information Act 2002 (NT); Information Privacy Act 2000 (Vic); Health Records (Privacy and Access) Act 1997 (ACT); Health Records and Information Privacy Act 2002 (NSW); Personal Information Protection Act 2004 (Tas); Health Records Act 2001 (Vic); Recommendations for introducing information privacy legislation in Western Australia: Office of the Attorney-General for Western Australia, Privacy Legislation for Western Australia Policy Research Paper (2003) referred to by David Lindsay An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law
(2005) *Melb. U. L. Rev.* 1.
[30] L A Bygrave *Data privacy law: An international perspective* (2014) 119.
[31] S Warren & L Brandeis The Right to Privacy (1890) 4 *Harvard Law Review* 193.
[32] D Solove The Origins and Growth of Information Privacy Law (2003) 748 *PLI* 53-6.

permitted to overstep …'[33] According to Alan Westin, privacy is the ability to control the information others have about you.[34] In accordance with the above philosophical views, it is an affront to ones privacy for an unauthorised opening, to read, divulge or record a person's a person's email and internet activities or eavesdrop on her conversations without permission or lawful excuse. It is also unlawful to appropriate or misappropriate another person's information for commercial purposes without permission. Privacy exist in terms of 'ability to control the information others may have about you', to restrict physical access to oneself and limit access to intimate sensitive information about oneself.[35] This is so for several reasons; control over one's privacy enhances the sense of one's dignity and self-worth; it enhances the development of individual personality without manipulations by others while a sense of personal autonomy enables individuals create and maintain different social relationships.[36] In many countries, the concept has been fused with data protection, which interprets privacy in terms of managing personal information.[37]

2.1.1. The right to privacy in international law

The right to privacy is enshrined in standard-setting human rights instruments like the Universal Declaration 1948, art 12,[38] the International Covenant 1966, art 17[39] and other international human rights instruments,[40] several soft laws and Declarations. The International Covenant,[41] art 17 provides as follows:

[33] J S Mill *Principles of Political Economy with Some of their Applications to Social Philosophy* 1965) 938.
[34] A R Miller *The Assault on Privacy: Computers, Databank and Dossiers* 1971 at 25; A Westin, *Privacy and Freedom* 1 ed 1967 7.
[35] O O Salami Privacy Protection For Mobile Health (Mhealth) In Nigeria: A Consideration Of The EU Regime For Data Protection As A Conceptual Model For Reforming Nigeria's Privacy Legislation Submitted in partial fulfilment of the requirements for the degree of Master of Laws at Dalhousie University Halifax, Nova Scotia April 2015 21-25.
[36] Ibid at 25-27.
[37] D Banisar & S Davies Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments (1999) 18 *John Marshall Journal of Computer and Information Law* 1.
[38] G. A. res. 217 A(III), U.N. Doc. A/810 at 71 (1948).
[39] G. A. res. 2200A (XXI), 21 U. N. GAOR Supp. (No. 16) at 52, U. N. Doc. A/6316 (1966), 999 U. N. T. S. 171, entered into force March 23, 1976.
[40] Article 11 of the American Convention on Human Rights, Nov, 22, 1969, O. A. S. Treaty Series No. 36, at 1, OAE/Ser. L./V/II.23 doc. Rev. 2, entered into force July 18, 1978; the European Convention for the Protection of Human Rights and Fundamental Freedoms, art 8 213 U. N. T. S. 222, entered into force Sept. 3, 1953.
[41] The Covenant has been ratified by the greatest number of states. See Office of the United Nations High Commissioner for Human Rights, Status of Ratifications of the Principal International Human Rights Treaties as of 16 June 2006 available at http://www.ohchr.org/english/bodies/docs/RatificationStatus.pdf.

1. No one may be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence nor to unlawful attacks upon his honour and reputation.

2. Everyone has a right to the protection of the law against such interference or attacks.

The provision has been interpreted by the Human Rights Committee, the International Covenant's oversight body, in its General Comment 16 as a source of data protection principles applicable to both public and private entities.[42] According to the HRC:

> The competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. … The gathering and holding of personal information on computers, data banks and other devices whether by public bodies or private individuals, and bodies must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. …

The HRC's Comment also covered the right of every person (or data subject) to have access to information held of them by public authorities and to correct whatever errors contained therein.[43]

However, the problem with HRC's General Comments is that they are not binding on States though they are authoritative expositions of the International Covenant.[44] Even citizens of States that have ratified the First Optional Protocol to the International Covenant may only bring complaints against such States before the HRC after exhausting all domestic remedies. Most importantly, the case law developed on art 17 reflect, but do not measure up to data protection principles as stated in international instruments such as the CoE Convention on data transfer and EU Directive on Data Protection.[45]

[42] General Comment 18, issued 23.3.1988 (Un Doc A/43/40, 181-183; UN Doc CCPR/C/21/Add.6; UN Doc/HRI/GEN/1/Rev 1 21-23), paras. 7 & 10.
[43] Ibid.
[44] The International Covenant, art 40(4).
[45] Bygrave n 28 at 258.

Nevertheless, veritable data protection principles are also deducible from the common agreement of states under art 2(2) of the International Covenant whereby a State-party 'undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant'. The article enjoins each state Party to the present Covenant undertakes to take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant. This presupposes a positive obligation on States. Furthermore, a progressive understanding of the nature of rights within the United Nations is that the International Covenant imposes obligations on States to take concrete steps including through legislation to protect, respect and fulfil human rights.[46] Within this new conception, States have obligation *to respect* (not interfere with), but also *to protect* (put measures in place to prevent and remedy infringements of) and *fulfil* data privacy rights.

2.2. The normative basis for data protection

The normative basis for data protection principles is encapsulated in various international and regional standard-setting human rights treaties dealing with right to privacy such as the Universal Declaration of Human Rights 1948 ('the Universal Declaration')[47] and the International Covenant on Civil and Political Rights 1966 ('the International Covenant').[48] African countries too are beginning to pay more attention to data protection. By adopting the Convention on Cyberspace Security and Protection of Personal Data 2014 ('the CCSPPD')[49] the African Union signified its preparedness to promote an information society. The Council of Europe (CoE) Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the Free Movement of Such Data 1981 (Council of Europe 1981),[50] the European Community's (EC) Directive on Data Protection,[51] Privacy of Electronic Communications Directive (EU 2002/58/EC)[52] and the Organization for Economic

[46] Vienna Declaration and Programme of Action, adopted by the World Conference on Human Rights in Vienna on 25 June 1993, available at http://www.ohchr.org/Documents/ProfessionalInterest/vienna.pdf (assessed 29 March 2016).
[47] Universal Declaration op cit n 38.
[48] International Covenant op cit n 39.
[49] African Union Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV) available at https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf (accessed 24 March 2016).
[50] ETS No 108 adopted 28.1.1981, entered into force 1.10.1985, hereinafter the CoE Convention.
[51] Directive/95/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ No L 281, 23.11.1995, 31), adopted 24.10.1995.
[52] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (as further amended) concerning the processing of personal data and the protection of privacy in the electronic communications sector

Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data Convention 1981 (OECD 1981)[53] are some of the extant regimes. The basic essence of data protection principles stated in the CoE Convention, the EU Data Directive as well as laws emanating from them is to protect fundamental rights notably right to privacy.[54] Nigeria is signatory to the Universal Declaration, International Covenant (excepting its Optional Protocol) and the AU CCSPPD though it is yet to ratify any of them. This however does not detract from Nigeria's obligations to respect, protect and fulfil its international human rights obligations as dictated by the Vienna Convention on Human Rights.[55] Similarly, Nigeria is not bound by the European standards. There is however an emerging trend to comply with EU prescriptions of transboundary movement of personal data in terms of interconnectivity arrangements.[56] In recent times, the NCC has also looked towards Europe in fashioning anti-market domination[57] and interconnectivity rules.[58] The growing influence of the European Union Data Protection Directives in technologically advanced countries[59] including emerging data protection regimes in Africa[60] has also been observed. Moreover, global interconnectivity of telecommunication networks makes possible transfer of subscribers' personal information beyond the shores of Nigeria a foregone conclusion. It would therefore not be out of place to consider Europe's standards in this paper.

2.2.1. European Data protection principles

The discussion here focuses on principles sifted from major European data protection regimes mentioned above. Data protection laws first emerged in Germany before spreading across Europe and other parts of the world due to concerns for abuses inherent in digital

(Directive on privacy and electronic communications), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (accessed 29 March 2016). This Directive repeals the Telecommunications Data Protection Directive (97/66/EC) and obligates telecommunications companies, within the context of processing personal data to take extra measures against nuisance calls and protect confidentiality of communications and anonymity rights of callers.

[53] Hereinafter 'OECD Guidelines 1981'.

[54] See arts 1 of the CoE 1981 and EU Data Directive 1994.

[55] Op cit n 46.

[56] C B Opata Transplantation and Evolution of Legal Regulation of Interconnection Arrangements in the Nigerian Telecommunications Sector (2011) 14 *Int'l J. Comm. L. & Pol'y* 1-36.

[57] C. B. Opata Looking Towards Europe: Regulation of Dominance In Nigerian Telecommunications (2013) 14 *Competition and Regulation in Network Industries* 338-364.

[58] NCA 2003, ss 96-100.

[59] G Greenleaf The influence of European data privacy standards outside Europe: implications for globalization of Convention (2012) 2 *International Data Privacy Law* 68-92.

[60] A B Makulilo Data Protection Regimes in Africa: too far from the European 'adequacy' standard? (2013) 2 *International Data Privacy Law* 42-48.

transmission of personal information made possible by automated information and communication technologies.[61] Hence, Europe has one of the most well developed and up to date data protection regimes.[62]

Data protection principles in Europe are now fairly well established and prescribe general standards of protection for handling and processing of personal information by data controllers, processors and also in specific industries.[63] The principles require that personal data must be:

1. obtained fairly and lawfully;
2. adequate, relevant and not excessive to purpose of collection;
3. used only for the original specified purpose;
4. accurate and up to date;
5. accessible to the subject;
6. kept secure; and
7. destroyed after its purpose is completed.[64]

Bygrave[65] made a summary of data protection principles. Bygrave's summary correlate with Banisar and Davies' respectively as 'fair collection principle', 'minimality principle', 'purpose identification principle' and 'use limitation principle', 'data quality principle', 'individual participation principle' and 'security principle'.[66] Bygrave does not mention the 'destroyed after its purpose is completed' principle, but says every agency carrying out data processing must bear legal responsibility for every use to which data collected is put (accountability principle). [67]

The EU data protection model is based on 'enforceability', which ensures that data protection principles are enshrined in explicit laws and there is an independent entity styled 'Privacy Commissioner' to protect data subject's rights. But it can be argued that predictability is a

[61] D Banisar op cit, n 37.
[62] O O Salami op cit n 35.
[63] For example the EU Privacy of Electronic Communications Directives 2002/2/EC and 2002/58/EC apply specifically to processing of personal data in electronic communications services.
[64] D Banisar op cit, n 37 11.
[65] Bygrave, op cit, n 28.
[66] Ibid.
[67] Ibid.

function of enforceability, which ensure that rules accessible, serve legitimate interests and are compatible with aims of a democratic society (not subject to whims and caprices of data controllers). The EU Privacy of Electronic Communications Directive 2002, for example, regulates unsolicited direct marketing to all forms of electronic communications, unsolicited commercial (spam) and sms's to mobile telephones and provides a right of recourse in the event of unlawful processing. It also guarantees the right to withhold permission to use data in some circumstances.[68] The Directive ensures privacy of communications and internet use and that communication details are deleted once calls are terminated. The wide acceptance of the CoE Convention 1981, EU Data Directive 1995 and EU Telecommunications Directive 1997 (repealed by the Directive 2002/21/EC) in the Eurozone has spurred other countries' adoption of data protection laws in line with the European model. However, how privacy rights are limited in the European Union have been more extensively discussed in literature on art 8 of European Convention on Fundamental Freedoms and Human Rights.[69]

2.2.2. African model of data privacy

Not surprisingly, the AU CSSPPD – though a more expansive instrument – has borrowed significantly from the European model. But at the same time is commendable for underscoring African communitarian values in data protection strategies. However, the AU CSSPPD has not come into effect having not been ratified or domesticated by any African country.[70]

---

[68] F F Akinsuyi Nigerian Cyber Crime and Privacy Legislation, Time for Review (2010) 8 (downloaded from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1663633 on 29 March 2016).

[69] A comparison of art 8, ECHR and art 17 of international covenant reveals that art 8, which deals right to privacy in the European context is more explicitly worded than art 17. Art 8 provides thus:
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
The EU 'telephone interception cases' are the highlight the gist of art 8(2). A summary of jurisprudence of the European Commission and European Court of Human Rights on art 8(2) especially as regards the 'telephone interception cases' is that in limited circumstances the right to privacy protects a person's access to personal data held by public authorities. Moreover, enforcement of art 8 is carried out by the European Court of Human Rights (ECtHR) whose judgements are legally binding on all signatories to the ECHR. Similarly, art 10(1) also, in narrowly construed circumstances, recognises the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing and the right to withhold permission to use data in some circumstances. See Bygrave, op cit n 28.

[70] A comparative analysis of the AU CSSPPD and the EU data protection principles have been expertly carried out by L A Abdulrauf & C M Fombad African Union Data Protection Convention 2014: A possible cause for celebration of human rights in Africa? Paper delivered at the 2016 ICIL Conference held at Pretoria, South Africa on 22-23 February 2016 (paper on file with writer).

3. Data Protection in Nigerian Law and the NCC Regulations

This section problematises the Nigerian Constitution's underdeveloped state of legal protection for data privacy and engages with objectives underpinning the Nigerian SIM card registration policy ('the NCC Regulations') vis-à-vis the public interest in data protection. It argues that the fledgling safeguards in the NCC Regulations relating to phone subscribers' biometrics and personal data processing are weak, and offer little protection to privacy and other subscribers' rights in terms of recognised international standards. The adequacy of the Regulations is considered in light of some of the basic principles of data protection recognised above.[71]

3.1. Right to data privacy and the Constitution of the Federal Republic of Nigeria 1999

Nigeria is yet to enact a substantive or sectoral data protection law. To prepaid mobile phone subscribers in Nigeria as elsewhere, privacy, dignity and autonomy are crucial issues, hence the concern in this paper to ensure that adequate safeguards exist against potential abuses inherent in the application of the NCC Regulations. Few attempts to secure the much needed data protection rights of Nigerians can be found in the NCC's General Consumer Code of Practice for Telecommunications Services made pursuant to the Consumer Code of Practice Regulations in accordance with powers granted by s 21 of the NCA 2003.[72] The Code provides some protection for subscriber data collected by telecommunication companies. Essentially, these are broad and very limited efforts to protect the privacy of Nigerians (Salami 4). A Computer Security and Critical Infrastructure Protection Bill 2005 and Cybersecurity and Information Protection Agency Bill 2008 are currently considered by the national legislature.[73] The Nigerian Constitution guarantees the right to privacy under which the right to data protection may be subsumed. Section 37 of the Constitution of the Federal

[71] However, the extent to which prepaid SIM cards owners are entitled to anonymity from commercial advertisers and unsolicited contacts remains largely under-researched in literature and is not considered in detail in this paper.
[72] The Nigerian Communications Commission Consumer Code of Practice Regulations 2006, Schedule 1 (as may be amended from time to time).
[73] F F Akinsuyi op cit n 68 at 12-17.

Republic of Nigerian 1999[74] (the 1999 Constitution) which guarantees the right to privacy[75] provides as follows:

> The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.[76]

This constitutional provision encompasses freedoms of communication and of information, which are vital to a democracy, and secures those rights to Nigerians, but not necessarily foreigners. The right to privacy probably one of the most under-researched, under-litigated and under-developed rights in the Nigerian Constitution. The few instances in which recourse has been had to the right has been health-related cases. The instances involve the right of HIV-infected persons not to be discriminated against,[77] the duty of doctors not to disclose HIV status of infected clients to their sex partners[78] and the right of patents to informed consent.[79] The Nigerian Constitution is the grundnorm or yardstick for validity and operation of all other laws including international law, statutory provisions, rules of common law and equity.[80] In view of paucity of constitutional jurisprudence on data protection a person may have recourse to delict or common law torts of 'negligence', 'trespass to property', 'breach of confidentiality' or 'nervous shock' as a substitute for breach of privacy. However, the problem with tortuous actions is that a claimant must prove damage to be entitled to monetary compensation. But not so for claim for breach of human rights where damage is presumed. Arguably, s 37 protects data subjects in terms similar to what obtains under art 8 of the ECHR,[81] but this is still a very rudimentary aspect of Nigerian law. The low level of technological development might be responsible for under litigation of privacy rights in

[74] Cap C23 Laws of the Federation of Nigeria 2004. It came into effect on 29 May 1999. As discussed above, data protection principles may be found under the freedom of expression provisions (s 39), but is not explored further in this article.

[75] Privacy rights are also embedded in other human rights provisions of the Nigerian Constitution namely, right to freedom of religion (s 38) and freedom of expression (s 39), but the discussion focuses on s 37 – right to privacy.

[76] As discussed above, data protection principles may be found under the freedom of expression provisions (s 39), but is not explored further in this article.

[77] E Durojaye So sweet, so sour: A commentary on the Nigerian High Court's decision in Georgina Ahamefule v Imperial Hospital & Another relating to the rights of persons living with HIV (2013) 13 *AHRLJ* 464-480.

[78] B Odunsi Should Caregivers Be Compelled to Disclose Patients' HIV Infection to the Patients' Sex Partners? *Studies in Family Planning* (2007) 38 287-306.

[79] Y Z Lawal, E S Garba1, M O Ogirima et al The doctrine of informed consent in surgical practice (2011) 10 *Annals of African Medicine* 1-5.

[80] See the Constitution of the Federal Republic of Nigeria 1999 Constitution, ss 1 & 12.

[81] A Kusamotu Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European Union Directive 95/46 (2007) 16 *Information & Communications Technology Law* 155.

Nigeria, but considering being Africa's fastest growing telecommunications market the situation can no longer be tolerated. The lack of adequate data protection in Nigeria was decried by Ayo Kusamotu, who wrote:

> One finds that the National Information Technology Development Agency (NITDA, a sub-agency of the Nigerian Communications Commission, has developed a draft Nigerian Information Technology Policy, which was approved by the Nigerian Federal Executive Council in 2001. NITDA's IT Policy identifies some of its objectives as 'promot(ing) legislation (Bills and Acts) for the protection of on-line business transactions, privacy and security' and 'enhanc(ing) freedom and access to digital information at all levels while protecting personal privacy'. Until 2007, this remains a good intention insofar as privacy is concerned since, while a draft Cybercrime Act has been produced in Nigeria in 2003, no data protection legislation has been enacted in the approach favoured by EU 46/95 (footnotes omitted).[82]

For predictable regulation of an industry with rapidly changing technology such as telecommunications to be predictable there must assurance of regularity by means of a law upholding full-fledged rights of stakeholders. Therefore the next section analyses the NCC Regulations and the effect of paucity of data protection principles in its operation.

3.2. NCC Regulations: objectives, content and context

Prior to the roll out of mobile lines in 2001 no regulations or contractual requirement existed mandating identity verification of prepaid ('pay-as-you-go') subscribers of mobile telecommunication services either at point of sale or SIM card activation. Mandatory registration Regulations (NCC Regulations) were formalised in 2011 after a stakeholder consultative process. As explained on NCC website, the move for registration of SIM card users started in 2008 when security agencies approached the headship of the NCC for assistance in resolving the problem of identifying persons implicated in phone-related crimes. Registration policy was initiated on March 28, 2011 after an official flag-off ceremony performed in Abuja by the NCC Executive Vice Chairman, Dr. Eugene Juwah. Two basic prongs of mandatory registration policy are to make planning data available provide for the industry regulator and to combat the upsurge of 419 scams, kidnapping-related offences and terrorist activities, etc. The NCC Regulations was actually signed on 3rd day of November

[82] Ibid.

2011in terms of powers conferred on the Commission by section 70 of the NCA 2003 and all other powers enabling it in that behalf.

The Regulation itself lists four main objectives of SIM Registration namely,

1. To assist security agencies in resolving crimes and by extension to enhance the security of the state.

2. To facilitate the collation of data by the Commission about phone usage in Nigeria.

3. To enable operators to have a predictable profile about the users in their networks.

4. To enable the commission to effectively implement other value added services like Number Portability among others.[83]

Though SIM card registration officially ended in 2012 mobile operators are still expected to continue registering new subscribers who will only be able to make emergency calls unless registered.

Registration of Telephone Subscribers Regulations, 2011 (the NCC Regulations)

3.2.1. Data capture and creation of a Central Database

The Regulations call for creation of a central database for central processing of subscribers' "personal information" including full names, date of birth and gender, occupation and "biometric information" - finger prints and facial image of all subscribers - which have been registered as provided under s 11. The Database shall be segregated across network services so as to facilitate easy access persons authorised by the NCC.[84] Though it is to contain information compiled at network providers' own cost the Central Database shall be the sole property of the Government of Nigeria.[85] The Regulations do take cognisance that the sheer number of existing subscriber may necessitate the use independent contractors. Hence, 'data controllers' such as the Commission and network providers could employ an independent registration agent to carry out subscriber registration.[86]

[83] Nigerian Communications Commission 'Sim Registration' available on NCC website at http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=122&Itemid=113 (accessed 12 January 2016).
[84] NCC Regulations, s 4(3).
[85] NCC Regulations, s 5(1).
[86] NCC Regulations, s 9(3)(4).

3.2.2. Retention of information

The Regulations provides that a 'licensee 'shall have the right to retain and use its subscribers information on its network in accordance with the provisions of Part VI of the General Consumer Code of Practice for Telecommunications Services and any other instrument issued from time to time by the Commission.[87] It also contemplates a potential request for access to the central database or general request for information by the national security adviser and security agencies in the normal course of crime investigation. In this respect, s 8(1) provides that:

> Notwithstanding the provisions of these Regulations restricting access to Subscriber Information on the Central Database and subject to the provisions of any Act of the National Assembly, subscriber information on the Central Database shall be provided only to Security Agencies; provided that a prior written request is received by the Commission from an official of the requesting Security Agency who is not below the rank of an Assistant Commissioner of Police or a co-ordinate rank in any other Security Agency. (2) The written notice by the Security Agency pursuant to sub-regulation (1) of this regulation shall indicate the rank of the official of the requesting Security Agency and the purpose for which the information is required.

3.2.3. Privacy rights and safeguards against misuse of subscriber information

Certain provisions of the Regulations are very crucial provision in these regards. Section 9(1) is particularly pertinent because they recognised 37 of the Nigerian Constitution as the source of data protection rules. The section says that:

> In furtherance of the rights guaranteed by section 37 of the Constitution of the Federal Republic of Nigeria, 1999 and subject to any guidelines issued by the Commission including terms and conditions that may from time to time be issued either by the Commission or a licensee, any subscriber whose personal information is stored in the Central Database or a licensee's database, shall be entitled to view the said information and to request updates and amendments thereto. (2) The subscriber information contained in the Central Database shall be held on a strictly confidential basis and no person

[87] NCC Regulations, s 7.

or entity shall be allowed access to any subscriber information on the Central Database except as provided in these Regulations.

Sections 7 allows a licenced operator to retain and use subscriber information as may be permitted by the Commission, but sections 9 and 10 further enjoins licensees, independent registration agents and subscriber registration solution providers, and the Commission, when applicable to:

i) retain refrain from retaining, duplicating, dealing in or making copies of any subscriber information or storing it in any form or for any purpose other than as stipulated by the Regulations or an Act of the National Assembly;
ii) take independent action and all reasonable precautions pursuant to international best practices to preserve the integrity or unauthorised disclosure of subscriber information in the course of capturing or processing the information;
iii) utilise personal information retained solely pursuant to the Regulations, their operations, in accordance with the provisions of the General Consumer Code of Practice for Telecommunications Services, other instruments of the Commission and any Act of the National Assembly relating to use of personal information;
iv) not retain subscriber Biometrics after its transmission to the Central Database;
v) not release personal information to any person in breach of the Constitution or any other Act of the National Assembly;
vi) not release personal information subscribers to any third party, except security agencies, without obtaining the subscribers' prior written consent;
vii) not transfer any subscriber information outside Nigeria without the prior written consent of the Commission.

3.2.4. Penalties

The Regulations creates various offences and prescribes penalties for breaches of its provisions. For example, unlawful duplication, retention or dealing with subscriber information is an offence and attracts a penalty of N200, 000 (equivalent of $ 1000 US Dollars) per subscription medium.[88] Similarly, an entity that is 'found to have utilised a subscriber's information in any business, commercial or other transactions' is liable to a penalty of N1,000,000.00 (equivalent of $5000 US Dollars) per subscription medium.

[88] NCC Regulations, s 21(1).

3.3. Problems associated with the NCC Regulations

The right to privacy and data protection principles are not absolutes in that data protection laws may exempt government and private organisations from strict compliance with informational privacy for overriding public interests such as public safety, national security, the rights and freedom of others, crime control. Also, in a sales of SIM card purchase agreement, for example, a person may not have a reasonable expectation of privacy where he or she has 'ticked a box' authorising the use of his or her personal details for commercial purposes. International law makes an interplay between data protection and its exceptions. Restrictions must not be unlawful, unreasonable or arbitrary, but must be necessary in a democratic society and serve a legitimate purpose. It can be argued that limitation of data privacy must be within strict bounds of necessity and proportionality.

The potential adverse effects of SIM card registration schemes in Africa is a number of questions including the alleged link between crimes and use of mobile telephony.[89] The anonymity previously enjoyed by mobile telephone users in Africa has been increasingly eroded since 2006 due to adoption of mandatory registration of SIM cards by majority of industry regulators and governments in African countries including Nigeria.[90] The common argument in Africa and elsewhere[91] by proponents of registration is that criminals seeking anonymity are likely to use unregistered prepaid SIM cards. The counter argument, including available research evidence in Nigeria,[92] that such crimes are perpetrated by only a handful of people - sophisticated criminal networks - is equally plausible.

Mandatory registration directives and regulations usually provide for the processing – which involves the recording, storage and transmission - of raw personal data and information of subscribers. A sampling of mandatory registration procedures in three African countries, South Africa, Nigeria and the DR Congo conducted by Jentzsch is instructive.[93] It reveals that

[89] I. Kerr 'On the identity trail: Understanding the importance and impact of anonymity and authentication in a networked society'. Retrieved September 2007, from http://www.idtrail.org/; K Wallace *Anonymity, Ethics and Information Technology* (1999) 1, 23-35.
[90] Nicola Jentzsch Implications of mandatory registration of mobile phone users in Africa *Telecommunications Policy* (2012) 36 608.
[91] See Government of Switzerland. (2003). Conventions des Nations Unies pour la répression du financement du terrorisme et des attentats terroristes à l'explosif. Retrieved July 10, 2007, from http://www.parlament.ch/afs/data/f/rb/f_rb_20020052.htm; (Australian Communications Authority, 1997). Australian Communications Authority. (1997, December 22). ACA makes rule applying to pre-paid mobile services (Media Release No. 42 of 1997). Retrieved January 2016, from http://aca.gov .au/aca-home/media-releases/media_enquiries/1997/index.htm
[92] F Waziri *Advance Fee Fraud and Nigeria's National Security* (2007).
[93] N Jentzsch, op cit n 90.

subscriber identity module (SIM) card owners must supply certain information including their full names, proof of physical address, date of birth, residential address, residency status and means of identification to telephone companies to activate their SIM cards.[94] With the exception of Liberia, Nigeria is perhaps the only African country with enforced biometric data capture as part of its personal information registration procedure.[95]

As privacy rights defenders such as Gow argues, the claimed effectiveness of compulsory registration in crime deterrence is doubtful. Lattice concurs with Gow that mandatory registration 'is ineffectual in those cases for which it is claimed it is most needed'.[96] There are others who claim it amounts to an unlawful invasion of privacy to collect the identity information of whole populations, who have not committed any offence, while going after a handful of criminals.[97] In view of the above, there has been a call for a balancing of privacy rights with the needs of public safety and security.[98]

The enactment of black letters of rules though is a commendable first step towards data security in Nigeria is not enough deterrence against abuse for several reasons. Imposing biometrics registration on whole populations is excessive and amounts to a knee-jerk response by the State to inadequacies of crime control that are unrelated to mobile phone usage. The fact that the NCC does not yet possess the technology to monitor surreptitious transfer of data by the more technologically advanced telephone companies, cyber hackers and criminals gives cause for concern. Also, unauthorised sales of subscriber information may be made by telephone companies to advertisers who could send unsolicited and nuisance mails to subscribers. It is also feared that network service providers may disclose location data of subscribers to law enforcement agencies without due process.[99] The absence of a body independent of government in accordance with international best practices to mediate privacy rights between the NCC and telephone companies on one hand and subscribers, on the other, leaves a yawning implementation gap of the Regulations. While it may still be early to determine the overall effect of mandatory SIM card registration on privacy rights of mobile

[94] Ibid.
[95] K P Donovan & A K Martin, op cit n 25.
[96] J Lettice 'Swiss move to block al-Qaeda mobile phone supply. The Register. Retrieved April 14,2004,from http:// www.theregister.co.uk/2003/03/12/swiss_move_to_block_al/
[97] Office of the Privacy Commissioner of Canada. (2002). Privacy Commissioner's reply comments regarding the "Lawful Access" proposals. Retrieved January 15, 2016, from http://www .privcom.gc.ca/media/le_021125_e.asp; G A Gow & J Parisi Pursuing the Anonymous User: Privacy Rights and Mandatory Registration of Prepaid Mobile Phones. (2008) 28 *Bulletin of Science, Technology & Society* 61; N Jentzsch n 90 611.
[98] G A Gow & J Parisi, ibid.
[99] G A Gow Information privacy and mobile phones *Convergence* (2005) 11 75-87.

phone users in Nigeria, there is yet no data from law enforcement agencies as to percentage of crimes that are phone-related to justify the blanket measure. Furthermore, the veil of secrecy that traditionally surrounds law enforcement generally and national security in particular may ultimately becloud the future success of the Regulations.

Compulsory SIM card registration considering innovations in technological convergence is a threat to personal anonymity. The thinking that once data is secured in Central Data Bank to be housed at NCC headquarters is flawed. This is because of difficulties of regulating a technologically advancing industry like telecommunications whereby new technologies of data mining could easily render such data bases vulnerable to unauthorised access. National security agencies and the police could easily track a person's movements and compile information on private conversations and relationships, banking details, etc. Even when they possess lawful warrant to do so the necessary safeguards against misuse of information not connected to crime control activities, which may come into their possession has not been provided.[100] Considering the need for public safety and national security, the NCC Regulations has not addressed those narrow and exceptional circumstances when data may be retained or lawful interception of communications or transmission of information to third parties may only be carried out by judicial authorisation.[101] Predictability in regulating an industry underpinned by rapidly changing technology is critical for credibility of the regulator itself.

4. Conclusion and Recommendations

A rising digital economy such as Nigeria's calls for bold privacy protection. But in the absence of meaningful legal or constitutional safeguards, sectoral regulations such as the NCC Regulations are welcome, but are inadequate to protect and fulfil privacy expectations including data protection, dignity and other fundamental rights of subscribers. Despite the avowed goals of subscriber registration in Nigeria, the lack of a holistic legal framework to safeguard unlawful dealings in personal data of subscribers creates legal uncertainty as to subscribers rights and liabilities vis-à-vis the State, the NCC, technologically advanced telephone companies and other data controllers in cases of unlawful data retention and illegal dealings. Considering the claimed ownership by the Federal Government of Nigeria to the Central Database of subscribers' biometrics and personal data there need for an intermediary

[100] The NCC is considering the adoption of formal guidelines on interception of communications for national security.
[101] G A Gow & J Parisi, op cit n 98.

body to step in and protect over 180 million Nigeria yearning for modern communication services. In the unlikely event of an immediate amendment to the Constitution to create a right to informational or data privacy, there is need for urgent enactment of a data protection law by relevant national authorities.