Acronyms and abbreviations

ACHPR	African Charter on Human and Peoples' Rights
APEC	Asia-Pacific Economic Cooperation
AU	African Union
BVN	Bank Verification Number
CBN	Central Bank of Nigeria
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSA	Canadian Standards Association
DPA	Data Protection Agency/Authority
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECOWAS	Economic Community of West African States
EEC	European Economic Community
EPIC	Electronic Privacy Information Centre
EU	European Union
FIPs	Fair Information Principles/ Fair Information Practices
FOIA	Freedom of Information Act (Nigeria)
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
INEC	Independent National Electoral Commission
IT	Information Technology
LFN	Laws of the Federation of Nigeria
NCA	Nigerian Communications Act
NCC	Nigerian Communications Commission
NIMC	National Identity Management Commission
NITDA	National Information Technology Development Agency
NSA	National Security Agency (US)
OAU	Organisation of African Unity
OECD	Organisation for Economic Cooperation and Development
P3P	Platform for Privacy Preferences
PbD	Privacy by Design
PET	Privacy Enhancing Technologies

PI	Privacy International
PIA	Privacy Impact Assessment
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
POPIA	Protection of Personal Information Act (South Africa)
PVC	Permanent Voters Card
SADC	Southern African Development Community
SALRC	South African Law Reform Commission
SCC	Supreme Court of Canada
TBDF	Transborder Data Flow
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations
WP	Working Party

Abstract

The thesis examines the legal protection of data privacy in Nigeria. Investigating this issue is crucial in the wake of the rise in data processing activities as a result of the relative advances in technology which challenge human rights. Generally, the right to data privacy emerged because of the need to protect individuals from risks resulting from the automated or manual processing of their personal information. Unlike the general assumption in most data privacy literature, however, this study considers data privacy as a *sui generis* right with an 'added-value' beyond the traditional the right to privacy.

The thesis, therefore, argues that the extant legal framework in Nigeria is manifestly inadequate to effectively protect individuals from the threats resulting from the processing of their personal information. This view is held based on an analysis of the major data privacy issues in Nigeria today and a review of the current legal regime. Thus, scholarship that contends that there is insufficient processing in the country which is a reason why data privacy right is neglected is challenged. Furthermore, the thesis argues that useful lessons can be obtained from Canada and South Africa for the purpose of improving the data privacy regime in Nigeria, although, it is admitted that both regimes are not perfect. Therefore, with the aid of a combination of descriptive, analytic and comparative methods, an in-depth study is carried out of the Canadian and South African legal regimes on data privacy protection. In carrying out this study, the focus is placed on the constitutional and statutory mechanisms for data privacy protection. The statutory mechanism in this case is the comprehensive data privacy code. In addition, the thesis brings together contemporary debates on improving data privacy regimes and a 'rights-based' approach is proposed for Nigeria. This is because, data privacy protection in African countries is usually misconceived as basically for economic purposes without due regard to human rights and fundamental freedoms. In conclusion, the thesis contends that, contrary to the common belief, merely enacting a legislation, which is a 'cut and paste' of foreign data privacy laws, is not a silver bullet to resolving the data privacy problem in Nigeria. The thesis, therefore, recommends an effective legal regime based on insights from the Canadian and South African experiences. Similarly, other pragmatic ways of effective data privacy protection in Nigeria are suggested such as improving awareness and scholarship, strengthening the judiciary and improved cooperation with international and regional data privacy regimes.

Keywords: data privacy, data protection, privacy, human rights, *sui generis* right, Nigerian legislation, comprehensive law, rights-based approach, international data privacy law, legal reforms.

Table of contents

Chapter one

General introduction

1.1. Background

…data protection [data privacy] is also emerging as a distinct human right or fundamental right.[1]

Nigeria is a country that is making significant strides in terms of the access and usage of information and communication technology (ICT).[2] This development, though laudable, poses significant challenges to human rights and fundamental freedoms.[3] One such challenge is the incessant (and sometimes inadvertent) violation of the peoples' right to data privacy. Recently in Nigeria, the activities of various entities with regard to the personal information of individuals, aided by advances in technology, amounted to a violation of data privacy. Data privacy, basically, is the right of individuals to control the processing of their personal information so that it is used only for the purposes they

1 Statement credited to Martin Scheinin, the United Nations (UN) Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2005-2011). See 'Reports by UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' 28 December 2009 A/HRC/13/37 available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf (accessed 1 November 2015) 6.

2 F Odufuwa *What is happening in ICTs in Nigeria: A supply-and demand-side analysis of the ICT sector* (2012) 42. See also ITU 'Measuring the information society report' (2014) available at https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf (accessed 1 November 2015).

3 See generally B Owasanoye & O Akanle 'ICTs, freedom of information and privacy rights in Nigeria: A legal analysis' (2010) 16(1) *East African Journal of Peace & Human Rights* 99-123.

desire.[4] Processing, in this regard, includes various activities performed with regard to their personal information such as its collection, storage and dissemination.[5]

Indeed, the current 'information revolution'[6] has brought issues of data privacy into the limelight. Data privacy is so crucial today that it has dominated the policy agenda of many international human rights and economic institutions.[7] It is, similarly, increasingly attracting the attention of policymakers, academics, national security agencies and legislators all around the world.[8] In fact, there have, lately, been strong arguments in support of the fact that the *sui generis* right has 'crystallized into a norm of customary international law.'[9] Perhaps, this is the reason why Kuner observes that data-privacy-related issues are 'destined to remain one of the most important regulatory and policy issues of the 21st century'.[10] This shows that data privacy is a topic that is difficult to ignore at both national and international levels, especially given the so-called 'information society'. The importance of the subject, however, appears not to be appreciated sufficiently in Nigeria.

---

4 See RK Zimmerman 'The way the "cookies" crumble: Internet privacy and data protection in the twenty-first century' (2002) 4 *Legislation and Public Policy* 442. Zimmerman relied on other scholars for this definition and argues that data protection (data privacy) is a category of privacy also called *information privacy*. Other scholars like Schartum reject such contention. See DW Schartum 'Designing and formulating data protection laws' (2008)18 *International Journal of Law and Information Technology* 2.

5 The word 'processing' has a very broad connotation to include all kinds of activities performed in relation to personal information. A commentator, therefore, contends that 'it is difficult to conceive of any operation performed on personal data in electronic commerce which would not be covered by it.' See C Kuner *European data protection law: Corporate compliance and regulation* (2007) 74.

6 The definition of information revolution is contextual. In the context of this thesis, 'information revolution' is a term used to describe the proliferation and availability of information and the accompanying changes brought about by its processing (storage and dissemination) as a result of advances in computers, the internet, and other electronic devices. This development is usually stated to have begun in the 20th century. See *Oxford English Dictionary* http://www.oxforddictionaries.com/definition/english/information-revolution (accessed 1 November 2015). Nevertheless, economist like Wilson defines information revolution as a process through which ICTs are produced, distributed, and consumed across the globe. In this regard, ICTs are perceived to be valuable business resources such as land and capital. See EJ Wilson III *The information revolution and developing countries* (2006) 3.

7 Indeed, Kuner observes that 'the globalization of data processing and the Snowden revelations that came to light in the summer of 2013 have led to an increased interest in regulating data protection at the international level.' See C Kuner 'The European Union and the search for an international data protection framework' (2014) 2(1) *Groningen Journal of International Law* 55. See also L Kong 'Data protection and transborder data flow in the European global context' (2010) 21(2) *The European Journal of International Law* 442.

8 M Zalnieriute 'Book review: Paul Bernal, Internet privacy rights: Rights to protect autonomy' (2015) 31 *Computer Law and Security Review* 312-313.

9 M Zalnieriute 'An international constitutional moment for data privacy in the times of mass surveillance' (2015) 23 *International Journal of Law and Information Technology* 99-133.

10 C Kuner *European data privacy law and online business* (2003) xi.

Lately, developing countries like Nigeria are beginning to experience, first-hand, the myriad issues brought about by personal information. Firstly, personal data/information is now an extremely valuable commodity which has been aptly described as the lifeblood and basic currency of the information economy.[11] This has made it increasingly sought by various entities without, in many cases, regard to the rights of the individuals who are the subject of the data. Secondly, there is a difficulty in comprehending the exact purpose or value of data privacy in African countries (in general) and Nigeria (in particular).[12] According to Makulilo, data privacy in African countries is basically perceived as being confined to economic purposes, and this has been a driving force in enacting data privacy laws across Africa.[13] This is problematic from the perspective of human rights because an individual's personal information is an embodiment of, or a facet of, his/her personality since it is capable of telling a story about him/her.[14] Understood from this perspective, if our personal information is as good as ourselves in real terms, it ought, then, to be accorded the necessary human rights protection so that sufficient control can be exercised over its processing.[15] Neethling's view is apt in this regard, as he contends that:

---

11 N Robinson *et al* 'Review of the European Data Protection Directive' (Technical report), RAND Corporation (May 2009) 12 available at http://www.rand.org/pubs/technical_reports/TR710.html (accessed 1 November 2015). They authors adopted the word 'currency of the internet economy' from 'OECD Ministerial Meeting on the Future of the Internet Economy' available at http://www.oecd.org/document/8/0,3343,en_2649_34487_40863240_1_1_1_1,00.html (accessed 1 November 2015).

12 AB Makulilo 'Protection of personal information in sub-Saharan Africa' published *Dr Jur* thesis, University of Bremen, 2012 469.

13 Makulilo (n 12 above) 469.

14 See G Zanfir 'The right to data portability in the context of the EU data protection reform' (2012) 3 (2) *International Data Privacy Law* 151. She argues that '[t]he amounts of data, especially when combined can be seen as a continuation of one's personality in the digital world, creating a digital personality of the individual.'

15 It is based on this philosophy that some scholars advocate property rights in personal information. See generally N Purtova 'Property rights in personal data: Learning from the American discourse' (2009) 25 *Computer Law & Security Review* 507-521; N Purtova *Property rights in personal data: A European perspective* (2012); and DJ Solove 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 53 *Stanford Law Review* 1446. Indeed, the law of intellectual property (especially, copyright) and data privacy law have a certain kind of relationship because of the contention that personal information is an individual's intangible property and thus, confers intellectual property rights on such an individual. However, in recent times, such a relationship has not been so cordial especially with regard to Digital Rights Management (DRM). See Article 29 Data Protection Working Party 'Working document on protection issues related to intellectual property' January 18, 2005 available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp104_en.pdf (accessed 24 January 2016). It is noteworthy that intellectual property rights could be in the form of copyright, trademark, patents and confidential information. Copyright is the right of intellectual creators in their creation. It mainly protects the form of expression of ideas and not the ideas themselves. Ideas may, however, be protected as confidential information. A trademark is a sign or design that personalises the products or services of an enterprise and distinguishes such products from that of its competitors. Patent is a right (or a document creating such right) over an invention which creates a legal situation whereby the patented invention can only be

> [s]ince as a rule individuals attach considerable significance to facets of their personality – so much so that most personality rights have also been entrenched as human rights – and are accordingly sensitive to infringements thereof, it can as premise be accepted that all legal systems strive towards, and indeed have an obligation, because of their human rights connotation, to provide for comprehensive personality protection.[16]

The threats to individuals brought about by the processing of their personal information (also referred to as the personal information or data processing problem)[17] is usually discussed in relation to technological developments,[18] although scholars, like Purtova, contend that this problem is also motivated by institutional, market and societal developments.[19] Without a doubt, the on-going digitalisation of many African economies, especially that of Nigeria, makes this investigation focused largely on the effects of advances in technology on the data privacy of individuals. This by no means, however, undermines other developments identified by Purtova. The internet and other ICTs are now inevitable tools in the lives of many people in Nigeria. This view is justified by the fact that Nigeria has one of the highest populations of internet users in the world.[20] The Nigerian Minister for communication technology recently stated that the country had recorded a fifty two percent (52%) internet growth rate and a rapid increase in the 'adoption and use of ICTs to automate some operations and processes of government Ministries, Departments and Agencies.'[21] Similarly, Nigeria has recently been described 'as [a] country with the highest potential for Information and Communication Technology

---

exploited with the authorisation of the owner of the patent. See generally World Intellectual Property Organisation (WIPO) *WIPO intellectual property handbook* (2004). It is submitted that in as much as any of these intellectual properties contain information relating to an identifiable person, then it will be a subject matter of data privacy law.

16 J Neethling 'Personality rights: a comparative overview' (2005) 38(2) *Comparative and International Law Journal of Southern Africa* 211.

17 Purtova *Property rights in personal data: A European perspective* (n 15 above) 17.

18 GG Fuster *The emergence of personal data as a fundamental right of the EU* (2014) 5.

19 Based on Purtova's ideas, institutional developments which cause personal information problems are developments in public and private entities which increase their reliance on personal information. With regard to market related development, Purtova referred to the increasing commodification of personal information where it is traded for various purposes. A societal development, on the other hand, is the increasing need of humans, as social animals, to learn about others and tell others about themselves. This results in the proliferation of Social Networking Services (SNSs). Purtova (n 15 above) 18. In my view, however, all these developments can also be arguably said to be facilitated by advances in technology.

20 See 'Internet usage on Nigeria's telecoms networks hits 93 million –NCC' *Leadership* 12 September 2015. See discussions in chapter 3 (3.2).

21 E Amaefule 'Nigeria recorded 52 % internet growth in 2014 – Minister' *Punch* 18 May 2015. Similarly, as of July 2015, the NCC estimated the total number of internet users in Nigeria to be more than 93 million.

investment on the African continent.'[22] Nigeria today records a very heavy presence online in various e-commerce platforms such as online shopping and e-banking.[23] In fact, it was recently reported that the country has an estimate of over two million US Dollar worth of e-commerce retail transactions weekly.[24] Similarly, a number of governmental services are, in recent times, being offered online with e-government initiatives.[25] Both government and commercial services are increasingly rendered with the aid of personal information processing. This significant leap in the application of ICTs in Nigeria increases the availability and ease of the accessibility to personal information with consequences which are sometime dire for human rights and fundamental freedoms.[26]

The negative effects of the processing of individuals' personal information *sans* significant legal protection are no longer in contention. Concerns have been widely expressed regarding these effects.[27] Bennett, however, contends that the harm resulting from computerised data processing 'is not immediately obvious.'[28] Roos expresses the fear that personal information being processed may be: inaccurate, incomplete or irrelevant; accessed or disclosed without authorisation; used for purposes other than that for which they were collected or destroyed.[29] In a more structured manner, Purtova, relying on Zarsky, analysed the concerns based on the various stages of data processing.[30] In the data

---

22 MA Araromi 'Regulatory framework of communication sector: A comparative analysis between Nigeria and South Africa' (2015) 23(2) *African Journal of International and Comparative Law* 274.

23 AO Oyewunmi 'The ICT revolution and commercial sectors in Nigeria: Impacts and legal interventions' (2012) 5 *British Journal of Arts and Social Sciences* 235.

24 S Sebatindira 'A glimpse into the emergent e-commerce in Nigeria' http://www.consultancyafrica.com/index.php?option=com_content&view=article&id=1754:a-glimpse-into-the-emergent-e-commerce-in-nigeria&catid=82:african-industry-a-business&Itemid=266 (accessed 1 November 2015).

25 See D Akunyili 'ICT and e-government in Nigeria : Opportunities and challenges' address by the Hon. Minister of Information and Communications, Prof Dora Akunyili, at the world congress on information technology, Amsterdam, the Netherlands, 25th-27th May 2010 available at https://goafrit.wordpress.com/2010/06/12/ict-and-e-government-in-nigeria-prof-akunyili/ (accessed 1 November 2015).

26 Indeed, it has rightly been stated that the question today is not whether information can be obtained but rather whether it should be obtained and where it is obtained, how it should be used. See South African Law Reforms Commission (SALRC) 'Privacy and data protection report' (2009) vi available at http://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf (accessed 1 November 2015).

27 For an in-depth analysis of these concerns with particular emphasis on databases, see Solove (n 15 above).

28 CJ Bennett *Regulating privacy: Data protection and public policy in Europe and the United States* (1992) 12.

29 A Roos 'The law of data (privacy) protection: A comparative and theoretical study' unpublished LLD thesis, University of South Africa 2003 6.

30 Putrova (n 15 above) 44. TZ Zarsky 'Desperately seeking solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society' (2004) 56(1) *Maine Law Review* 15.

collection process, the main issues identified are issues of secrecy, imbalance in power and autonomy.[31] With regard to the data analysis stage, the main concerns relate to fear of errors, misrepresentation, dehumanisation and aggregation.[32] The final stage is the implementation of data and the main threats are the possibility of discrimination, manipulation and inequality.[33] Other authors, like Birnhack,[34] Bernal[35] and Neethling,[36] focused more on human rights concerns such as the effect of (unlawful) data processing on dignity, autonomy and personality. All these concerns can, debatably, also be attributed to data processing activities in Nigeria.

In spite of these widely acknowledged concerns,[37] data privacy has, arguably, not received the desired attention in Africa unlike other parts of the world. Scholars have advanced various reasons for this unhappy state of affairs. The main explanation is that Africans tend to underestimate the risks resulting from the processing of their personal information.[38] It must, however, be stated that, notwithstanding this, some African countries are beginning to recognise the value of data privacy.[39] Such is also the case at regional and sub-regional

---

31 Putrova (n 15 above) 45-47;

32 Putrova (n 15 above) 47-50.

33 Putrova (n 15 above) 50-51.The learned scholar also identified some other concerns, such as a lack of transparency and accountability in data flow.

34 Birnhack worries more about the effect data processing has on human dignity. He contends that 'the control of personal data is a matter of human dignity. A person should be treated as a moral, independent agent capable of deciding his or her own path in life.' MD Birnhack 'The EU Data Protection Directive: An engine of a global regime' (2008) 24(6) *Computer Law & Security Report* 509.

35 P Bernal *Internet privacy rights: Rights to protect autonomy* (2014). See also Tzanou where she argues that 'data protection is not simply about informational privacy; it is about informational *autonomy*.' M Tzanou 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right' (2013) 3(2) *International Data Privacy Law* 89. (Emphasis added).

36 Neethling, before the enactments of the POPIA, earlier contended that 'in view of the extent and seriousness of the threat to an *individual's personality*, it is surprising to find that under South African law – unlike the position in many other legal system – measures for the protection of individual (data protection) are very scant.' J Neethling *et al Law of personality* (2005) 217. (Emphasis added).

37 Although some scholars undermine these concerns as not being supported with factual evidence but rather speculative in nature. See for example, L Bergkamp 'The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy' (2002) 18(1) *Computer Law & Security Report* 31-47.

38 EM Bakibinga 'Managing electronic privacy in the telecommunication sub-sector: The Ugandan perspective' (2004) http://www.thepublicvoice.org/events/capetown04/bakibinga.doc (accessed 1 November 2015).

39 It has been reported that, as at October 2015, 16 out of 54 African countries have data privacy legislation and several have draft bills pending in the legislative assemblies. See AB Makulilo 'Privacy in mobile money: Central banks in Africa and their regulatory limits' (2015) 0 *International Journal of Law and Technology* 9. This may be the result of advances in ICT in Africa which has been acknowledged by JT Murphy & P Carmody *Africa's information revolution: Technical regimes and production networks* (2015).

levels where we find various data privacy instruments springing up.[40] Unfortunately, the same cannot be said of Nigeria, where data privacy issues seem to be totally neglected or ignored.[41] This is so in spite of a number of recent activities which shows significant threat to individuals' right to control the use of their personal information. For example, there is currently an effort by the government to integrate personal information records of different agencies in Nigeria with the attendant ease of aggregation of personal information.[42] Similarly, there is a sharp increase in surveillance activities by the Nigerian government.[43] All these imply substantial loss of control by the people over the use of a significant aspect of their personality. The implication of some of these activities, are, however, far from being appreciated in Nigeria. From the human rights perspective, this study brings to the fore a number of salient issues with regard to data privacy in Nigeria and how effective protection can be realised.

The study proceeds from the assumption that personal information has an inherent value and, therefore, individuals need to be protected from the effects of its processing. It is, furthermore, hinged on certain other key hypotheses based on the current data privacy literature, firstly, that data privacy, like privacy, is a human right although it has its economic dimension. Nigerians are, therefore, also entitled to this human right protection. Secondly, although data privacy has its roots and normative basis in the right to privacy, it has an 'added-value' beyond the scope of the traditional right to privacy especially in this digital age. Thirdly, constitutional and statutory (comprehensive law) mechanisms are the

---

40 See generally D Banisar 'Linking ICTs, the right to privacy, freedom of expression and access to information' (2010) 16 (1) *East African Journal of Peace and Human Rights* 136. AB Makulilo 'Myth and reality of harmonization of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 78-89.

41 LA Abdulrauf 'Do we need to bother about protecting our personal data? Reflections on neglecting data protection in Nigeria' (2014) 5(2) *Yonsei Law Journal* 67-95.

42 The President of Nigeria, Muhammadu Buhari, only recently called on the Independent National Electoral Commission (INEC), Federal Road Safety Commission (FRSC), and the National Population Commission (NPC) to harmonise their personal data processing initiatives so as to facilitate the more effective use of the personal information. See 'Buhari orders INEC, FRSC, NPC to harmonise biometric data' *Vanguard* 11 August 2015. Indeed, Solove points out the problem of aggregation specifically which he calls the 'aggregation effect'. He notes that '[t]he digital revolution has enabled information to be easily amassed and combined. Even information that is superficial or incomplete can be quite useful in obtaining more data about individuals. Information breeds information.' DJ Solove *The digital person: Technology and privacy in the information age* (2004) 44. Thus '[i]t is the totality of information about a person and how it is used that poses the greatest threat to [data] privacy.' Solove (n 15 above) 1452.

43 For example, it was recently reported that the Nigerian government is spying on its citizens by collecting personal information from their telephone conversations with the aid of sophisticated ICT devices. M. Mojeed, 'EXCLUSIVE: Nigerians Beware! Jonathan procures N11 billion equipment to tap your phones', *Premium Times* (Nigeria), 26 February 2015, available at http://www.premiumtimesng.com/news/headlines/177557-exclusive-nigerians-beware-jonathan-procures-n11-billion-equipment-to-tap-your-phones.html (accessed 1 November 2015).

most effective legal instruments for the protection of data privacy. Fourthly, although most (if not all) data privacy regimes are 'legal transplants'[44] of international (regional) data privacy instruments, vital insights can still be gained from a careful study of the regimes of specific countries. Fifthly, a 'rights-based' approach may be more effective in realising the right to data privacy in Nigeria.

1.2. Problem statement, objectives and justification of the study

1.2.1. Problem statement

Nigerian policymakers are yet to understand the human rights implications of the unfair and unlawful processing of the people's personal information. Data privacy is yet to be given significant attention in Nigeria in spite of the considerable global interest it has gained.[45] There is still no coherent legal regime for the protection of data privacy as narrowly construed.[46] This is so in spite of the rising incidents of identity thefts[47] and data breaches.[48] The extant legal framework, which merely protects secret or private information, arguably cannot cope with the modern-day 'personal information problem' which affects the public as much as the private information of individuals. From this perspective, while the interest of individuals in protecting 'their hidden worlds' cannot be undermined, there are contemporary threats to their personal information which goes

---

44 G Greenleaf *Asian data privacy law: Trade and human rights perspective* (2014) 12-13.This term 'legal transplants' is used by Siems to describe one of the modern methods of comparative research methodology which involves 'legal borrowing' from the laws of other jurisdiction. See MM Siems *Comparative law* (2014)192; see also M Graziadei 'Comparative law as the study of transplants and receptions', in M Reimann & R Zimmermann (eds) *The Oxford handbook of comparative law* (2006) 456-461.

45 Somewhat ironically, Nigeria was one of the countries who endorsed the UN Human Rights Council's Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet in July 2012. See MC Kettemann, 'The UN Human Rights Council Resolution on Human Rights on the Internet: Boost or bust for online human rights protection?' (2012) 1 *Human Security Perspectives* 145–169.

46 This is so in spite of the elaborate provisions in the Nigerian IT policy for the development of data privacy. Arguably, the document also conflates data privacy and privacy. Nigerian National Policy for Information Technology (IT) 'Use IT' available at http://www.functionx.com/nitpa/nigeria/ITPOLICY.PDF (accessed 1 November 2015).

47 It has been observed that identity thefts are part of the emerging ICT related crimes in Nigeria which need to be addressed urgently by the government. YI Arowosaiye, 'The new phenomenon of phishing, credit card fraud, identity theft, internet piracy and Nigeria criminal law' paper presented at the 3rd Conference on law and technology, Faculty of Law, University Kebangsaan Malaysia and Faculty of Law, University of Tasmania, Australia, 11 & 12 November 2008.

48 NA Nurudeen 'Nigeria: "Data Breaches cost increased to U.S. $3.8 Million in one year' *Daily Trust* 3 June 2015. Identity theft is a category of cybercrime which is punishable under the recent Cybercrime Act 2015. But the Act is a penal legislation and not a human right instrument. See also Owasanoye & Akanle (n 3 above) 113.

beyond threats to its privacy.[49] Thus understood, personal information, which may not necessarily be secret or confidential, also deserves independent protection because of the power it holds over individuals. This state of affairs, therefore, calls for profound legal reforms in this area. Policymakers in Nigeria, however, appear to be at a loss as to how such reforms should take place.

While there is a number of proposed data privacy legislation in Nigeria, the likelihood of their being able to influence effective data privacy protection remains doubtful. Presently, there are three draft bills which, arguably, contain basic data privacy principles - the Privacy Bill,[50] Data Protection Bill[51] and the Personal Information Protection Bill.[52] A number of issues can be raised with regard to these proposed laws which depict the level of government's commitment on data privacy protection. Firstly, these bills, as will be shown subsequently, are fundamentally weak when compared to the data privacy legislation in other jurisdictions. Similarly, questions arise as to the need for several bills which are poorly drafted within short intervals. There is, in addition, no evidence suggesting that any of these draft pieces of legislation have gone through sufficient debates and consultation such as are usually associated with law-making of data privacy legislation because of the complexities involved. In addition, the exact status of each of these bills remains largely unknown.

There are some non-binding data privacy instruments in the form of regulations, codes and guidelines in Nigeria. All these policies, apart from being like a 'patchwork quilt' are applicable only to particular government agencies. Furthermore, they lack coordination, which will naturally affect their implementation.[53] The existing soft law regime also provides individuals with limited protection because, firstly, they are generally non-binding legal instruments and, therefore, not as effective as a legislation. Secondly, there is no dedicated institutional mechanism to ensure compliance with these regulations.[54]

---

49 The general understanding that data privacy is all about concealment and secrecy is what Solove refers to as the 'secrecy paradigm' which he argues is the traditional understanding of privacy. See Solove (n 42 above) 42. See also Solove (n 15 above).

50 Privacy Bill 2009.

51 Data Protection Bill 2010.

52 The exact status of this Bill is unknown.

53 For example, Nigerian Information Technology Development Agency (NITDA) Guidelines on Data Protection (2013).

54 BO Jemilohun 'An appraisal of the institutional framework for data protection in the UK, USA, Canada and Nigeria' (2015) 1(1) *Journal of Asian and African Social Science and Humanities* 8-26.

These difficulties are further complicated by a generally poor level of awareness by a large section of the Nigerian populace.

Nigerian policymakers, and most scholars, seem to overlook the 'added-value' of a right to data privacy.[55] Similarly, their attention seems to be focused on the economic dimension of data privacy, especially from the point of view of the EU adequacy requirement and its implications for Nigeria's development. They seem also to believe erroneously that simply enacting a data privacy law is all that is needed for the realisation of data privacy right in Nigeria. This misconception misses certain important points with regard to data privacy and its regulation. Enacting a data privacy law is, without doubt, a necessary move towards realising data privacy protection. For effective realisation in a country like Nigeria, however, other crucial issues must be taken into consideration. A close examination of the present draft bills on data privacy shows that these important points are neglected. It is, therefore, arguable that, in the event that any of them is eventually enacted, it will join the collection of several other laws with little or no impact or *dead letter* laws.[56] In this regard, the Bill, if enacted, may hardly stand the test of time because decisive matters that are to be taken into consideration in the preparatory works are overlooked. In essence, while the lack of a coherent legal framework for the protection of data privacy is a problem, this is not the major problem in the area. The major problem is a lack of understanding of the personal information problem.

1.2.2. Objectives and justification of the study

In view of the issues raised above, the primary objective of this study is to investigate how data privacy can be protected effectively in Nigeria. This investigation is carried out based on lessons from an analysis of the Canadian and South African experiences. A study on issues of data privacy is significant at this stage of Nigeria's development for two reasons. Firstly, Nigeria is currently aspiring to take human rights protection to the next level because of its maturing democracy.[57] Subscribing to the hypothesis that data privacy is a

55 A ramification of this contention is found in an article by Jemilohun, where he contends that 'information about people is private to them and as such protection for privacy must of essence involve protection of their personal information.' See BO Jemilohun 'Legislating for data protection in Nigeria: Lessons from UK, Canada and India' (2010) 1(4) *Akungba Law Journal* 98. The author clearly overlooks the fact that there is much more to data privacy than protection of privacy.

56 The Black's law dictionary defines 'dead letter' law as 'a law or practice that, although not formally abolished, is no longer used, observed, or enforced.' See BA Garner *Black's law dictionary* 426.

57 See generally NS Okogbule 'Access to justice and human rights protection in Nigeria' (2005) 3(2) *SUR-International Journal of Human Rights* 94-113.

human right of contemporary significance will, therefore, make research in this area crucial. Secondly, it is beyond doubt that, because of the recent advances in the technology and the growing level of exposure to IT, IT related threats, such as cybercrime, identity thefts, phishing scams, and data breaches, have proliferated in Nigeria. A research of this nature is important as it increases awareness on data privacy and related issues which was earlier noted to be grossly lacking in Nigeria. Furthermore, while this study acknowledges existing works on data privacy in Nigeria, it adds a new dimension to this literature by looking at data privacy protection from a strictly human rights perspective (based on its human rights value).

1.3. Research questions

The primary question this study seeks to answer is: how can the protection of data privacy be realised effectively in Nigeria? In an attempt to answer this broad research question, some sub-questions will be addressed:

1. How has the *sui generis* right to data privacy developed through international and regional instruments?
2. To what extent is the *sui generis* right to data privacy recognised and protected under the extant Nigerian legal framework?
3. What legal framework (constitutional and statutory) protects data privacy in Canada and South Africa?
4. What lessons can Nigeria learn from the Canadian and South African experiences on data privacy protection?
5. How can effective data privacy protection be realised in Nigeria using a rights-based approach?

1.4. Methodology of the study

In an attempt to answer the main question of this study, a desk research or 'library-based' method is adopted.[58] This means that both primary and secondary sources will be used for the purpose of the study. Primary sources that will be consulted are international and

[58] The research can also be said to be a doctrinal research method. See T Hutchinson 'Doctrinal research: Researching the jury' in D Watkins & M Burton *Research methods in* law (2013)7.

regional data privacy instruments,[59] constitutional provisions[60] and statutory data privacy codes of the selected countries.[61] Similarly, case laws also form an important primary source for the purpose of this research.[62] In addition, the study also relies heavily on secondary sources which include textbooks, published and unpublished dissertations, journal articles, preparatory works of legislation (*travaux préparatoires*), and conference and seminar papers.[63] Although the realisation of effective data privacy protection depends on the political will of the government and the level of awareness of the people, the quality of the legal framework also has a crucial role to play. The current state of the legal framework is captured sufficiently in these primary and secondary sources which makes the desk research method apt for this study.

For the purpose of obtaining useful lessons for Nigeria in realising effective data privacy protection, this research study will be both descriptive and analytical. In order to avoid the pitfalls of the study being merely descriptive, however, an evaluation is carried out of particular aspects of the data privacy regimes where value-judgments are made based on the researcher's understanding of the basic principles of data privacy law. This is so as to reveal both negative and positive aspects of these regimes. To put these lessons in an even better context, some comparative studies will be carried out. The comparison is important for two reasons. Firstly, it enables one to draw lessons from jurisdictions beyond Canada and South Africa (especially from the EU). Indeed, when it comes to any discussion on data privacy, it is very difficult to ignore the EU. In analysing the specifics of a data privacy regime in Canada or South Africa, therefore, comparisons will be made with what exists under the current (and proposed) EU regime on data privacy. Secondly, the

---

59 Organization for Economic Cooperation and Development (OECD) Guidelines, Council of Europe (CoE) Convention, European Union (EU) Charter, EU Directive, draft EU Regulation. Several other regional African instruments that will be consulted include the African Union (AU) Charter, AU Convention on Cybercrime and Data Protection and the Economic Community of West African States (ECOWAS) Supplementary Act on Data Protection.

60 The Constitution of the Federal Republic of Nigeria 1999, Canadian Constitution Act 1982, and the South African Constitution 1996.

61 The study focuses mainly on the two main Canadian data privacy laws. These are the Privacy Act and the Personal information Protection and Electronic Documents Act (PIPEDA). For South Africa, I will focus on the Protection of Personal Information Act (POPIA).

62 Especially in Canada where the data privacy regime is quite far more established that South Africa.

63 With regard to secondary sources, the OR Thambo law library at the University of Pretoria was useful in terms of access to literature. Nevertheless, the library of the University of South Africa was more useful with regard to texts on data privacy because of its very rich collection on data privacy law. I was granted full access to the library with the assistance of Professor Roos. Online materials were also very useful and were made available through the full access to the database of the University of Pretoria where journal articles were mostly downloaded. Online resources were, however, more useful when discussing data privacy practices in Canada. This is because of the free access to the website of the Canadian Office of the Privacy Commissioner. See www.priv.gc.ca.

comparison is important because the South African statutory data privacy code was passed into law only recently, and case law and literature are, thus, still developing. It is, therefore, thought that it is better to put the provisions of the South African data privacy law *vis-à-vis* an older and more mature EU data privacy regime. Moreover, the South African regime has been significantly inspired by the EU regime. On the whole, this study examines the data privacy framework of Canada and South Africa with a view to obtaining insight for Nigeria towards effective data privacy protection.

1.5. Scope and limitation of the study

This study looks specifically at the protection of data privacy in Nigeria. In this light, the thesis carefully considers only legal regimes that protect personal information as narrowly construed since they are the main concern of data privacy regimes. Legal frameworks that focus on privacy generally are, therefore, outside the scope of this work. This is because data privacy is now debatably a subject of law that can stand on its own, independent of privacy laws.[64] Privacy regimes (and literature) are considered only so far as they foster the *sui generis* right to data privacy or the protection of personal information. It is on this basis that certain constitutional and statutory provisions will be examined, especially because of the fact that data privacy (information privacy) is largely perceived as a sub-category of the right to privacy in the jurisdictions under focus. Nevertheless, the 'added-value' of a data privacy regime (above privacy) is the focus of this study. In addition, this thesis focuses only on constitutional and statutory protection of data privacy based on the assumption that both mechanisms are the most effective means of data privacy protection today.[65] With regard to statutory protection, the research is limited to the comprehensive data privacy law only. Comprehensive law is a special law that protects personal information as narrowly construed and contains all the fair information principles (FIPs).[66]

---

64 See LA Bygrave *Data privacy law: An international perspective* (2014) 1-8.

65 See J Neethling 'Features of the Protection of Personal Information Bill 2009, and the law of delict' (2012) 75 *Tydskrif vir hedendaagse Romeins-Hollandse Reg (THRHR)* 254-255. See also A Roos 'Data protection' in D Van der Merwe *et al Information and communications technology law* (2008) 358. Both scholars discuss the weakness of common law (law of delict) protection of personal information and the imperative of legislation.

66 A comprehensive data privacy law is, arguably, not defined by any scholar. I, however, take a leaf from one of Greenleaf's studies in defining a comprehensive law. He points out that '[a] [comprehensive] law must set out data privacy principles…in a special fashion, not only as a general constitutional protection for privacy, or civil action (tort) for infringement of privacy.' See G Greenleaf 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2014) 23(1) *Journal of Law, Information & Science* 8.

In seeking insights, the study does not consider sectoral law or laws that incidentally contain provisions on data privacy.[67]

Canadian and South African data privacy regimes stand out for a number of reasons which inform their selection for the purpose of lesson-drawing. For example, a recent report[68] by Privacy International (PI) and Electronic Privacy Information Center (EPIC),[69] *Privacy and human rights report*, rated Canada as one of 'the highest-ranking countries' in terms of data privacy protection.[70] Moreover, Canada's data privacy regime (private sector) is one of the very few that is deemed 'adequate', having obtained the EU approval stamp.[71] The point must, however, be made that the Canadian framework for data privacy is somewhat complex. There are different pieces of legislation at both the federal and provincial

---

67 Some sectoral laws are considered only in discussing Nigeria so as to establish the fact that data privacy is insufficiently and incoherently protected. Another instance where I considered sectoral laws important is in discussing data privacy protection in the Canadian health sector. Analysis was made of the Nova Scotia Personal Health Information Act because of the importance of protection of personal health information in Nigeria. Nevertheless, this isolated case does not go against the general rule of not considering sectoral laws because the health sector law is specifically for the protection of personal health information. It does not treat the protection of personal health information as merely incidental as is the approach of the Nigeria National Health Act. Similarly, the Act arguably contains all the basic FIPs.

68 See EPIC & Privacy International (PI) 'Privacy and human rights report' (2006) http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Contents.html (accessed 1 November 2015).

69 The US-based Electronic Privacy Information Center and the UK-based Privacy International have undertaken 'the most comprehensive' survey of global privacy ever published. This is *The privacy & human rights reports* which assess the state of surveillance and privacy protection in 70 countries. The most recent report at the time of this research is that published in 2007. It is said to be 'the most comprehensive single volume report published in the human rights field' with over 1,100 pages and more than 6000 footnotes. This report contains materials and commentary from more than 200 experts worldwide which include academics, human rights advocates, journalists and researchers. The report was used as a basis for a ranking assessment of the state of privacy (data protection) in all EU countries and 11 non- EU countries. The main objective of the project is two-fold, firstly, to recognise countries with effective privacy protection and respect for privacy for lessons to be learnt from their example from other countries, and, secondly, 'to identify countries which governments and privacy regulators have failed to create a healthy privacy environment.' See 'The 2007 International privacy ranking: State of privacy map' http://www.democraticunderground.com/discuss/duboard.php?az=view_all&address=132x3911587 (accessed 1 November 2015).

70 See EPIC & PI (n 67 above). See also RW London 'Comparative data protection and security law: A critical evaluation of legal standards' unpublished LLD thesis, University of South Africa, 2013 11; DH Flaherty 'Reflections on reforms of Federal Privacy Act' (2008) https://www.priv.gc.ca/information/pub/pa_ref_df_e.pdf (accessed 1 November 2015) 1. Though Flaherty argues that 'privacy international is blessedly unaware of, and/or turns a blind eye to, some of the least progressive aspects of the Canadian privacy law and practice, such as the antiquated Privacy Act and the lack of resourcing of privacy functions at federal government institutions.'

71 European Commission (EC) 'Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act' available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0002&from=EN (accessed 1 November 2015).

(territorial) level reflecting overlapping constitutional jurisdiction in the subject matter.[72] This seeming complexity is, however, not a shortcoming *per se* as it provides a very rich source of jurisprudence from which to draw insights. Another reason for the choice of Canada is the availability of, and accessibility to, scholarly works. This is more so with the robust and well-updated website of the Office of the Privacy Commissioner which contains much detail on the law and practice of data privacy protection in Canada.[73] Case laws,[74] decisions, presentations, speeches and publications of the Commissioner are all carefully uploaded and regularly updated on the website. All the resources contained in the website can also be accessed at no cost by academics all over the world. It can, therefore, be argued safely that the accessibility to these resources largely circumvents the need for field research.

The *privacy and human rights report* states that data privacy protection in South Africa is in the development phase, probably owing to the fact that, as at the time of the country studies, the South African data privacy law was still in the preparatory stage.[75] Although the law has now been passed, it remains untested having not fully come into force.[76] The South African data privacy regime, notwithstanding this, stands out for a number of reasons, which informed its selection for the purpose of this research study. Firstly, the Protection of Personal Information Act (POPIA) is a progressive document which contains elaborate provisions that tackle present and future data privacy challenges. Secondly, in terms of scholarship on data privacy in Africa, South Africa is one of the leading countries on the continent. Accessibility to literature, therefore, helps the understanding of the state of data privacy in South Africa and insights to be gained from them. Moreover, *travaux préparatoires* for the POPIA comprises very exhaustive discussions on the contents and interpretation of the Act.[77] The South African Law Reform Commission's *Privacy and data protection report*, which is, arguably, first of its kind in Africa, is publicly available

---

72 D Elder 'Canada' in M Kuschewsky (ed) *Data protection & privacy: Jurisdictional comparisons* (2012) 44. [There is a 2014 edition of this book which the researcher has unsuccessfully made attempt to get].

73 https://www.priv.gc.ca/

74 For case law, Canada also has a systematic and rich reporting system in websites like https://www.canlii.org/en/ and http://scc-csc.lexum.com/scc-csc/en/nav.do

75 EPIC & PI (n 68 above); London (n 70 above) 11.

76 Only certain sections have come into force. See Proclamation by the President of South Africa No. R. 25, 2014 available at https://www.saica.co.za/Portals/0/Technical/LegalAndGovernance/37544_pro25.pdf (accessed 1 November 2015).

77 SALRC (n 26 above).

and facilitates a research study of this nature which seeks to gain in-depth insight from the South African experience.

Beyond the quality of both the Canadian and South African regimes which makes for insightful discussions for Nigeria's purpose, other specific reasons also motivated the selection of both countries. One such motivation is the workability prospects for Nigeria. Factors that were put into consideration in this regard are, firstly, that both countries operate a federal system of government as is the case in Nigeria. The idea behind federalism is that powers are shared between the federal governments and states or federating units. This idea is relevant as it shows who has the responsibility to enact data privacy laws. Secondly, both Canada and South Africa, like Nigeria, belong to the Commonwealth and are all pluralistic societies.[78] All these go to show the prospects that both countries present in terms of the workability for Nigeria of the lessons obtained.

In substance, all data privacy laws are similar since they are all largely based on the same international documents.[79] There are, however, differences in little details which may have an effect on the overall realisation of the right to data privacy.[80] In this regard, Canada, being a member of the Asia-Pacific Economic Cooperation (APEC), is one of the few countries which have a data privacy legal framework relatively distinct from that of the EU. Moreover, the OECD Guidelines have been more influential in the Canadian data privacy framework than any other instrument. As such, quite a number of differences exist between the Canadian and EU data privacy regime.[81] The Canadian regime is said to achieve a balance between the American (*laissez-faire*) and the European (strict protectionist) approaches.[82] South Africa, on the other hand, belongs to both the African

---

78 Indeed, quite a number of authors have linked data privacy with culture. For example, Birnhack contends that Canada is a member of APEC which is a rival data privacy regime to the EU. APEC also seeks to balance right to privacy and commercial interest as does the EU. Its distinctive approach, however, is that it 'accords due recognition to cultural and other diversities that exist within its member economies.' Birnhack (n 34 above) 512. See also HN Olinger *et al* 'Western privacy and/or *Ubuntu?* Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa' (2007) 39(1) *International Information & Library Review* 31-43.

79 C Kuner 'An international legal framework for data protection: Issues and prospects' (2009) 25(4) *Computer Law & Security Review* 310. See also L Bygrave 'International agreements to protect personal data' in JB Rule & G Greenleaf (eds) *Global privacy protection: The first generation* (2008) 15.

80 Kuner contends that 'however, the differences in the cultural, historical, and legal approaches to data protection mean that once one descends from the highest level of abstraction, there are significant differences in detail.' Kuner (n 79 above) 310.

81 The most significant being the absence of strict restriction on transborder data flow in the Canadian law and the nature and scope of their data privacy regulatory bodies.

82 Jemilohun (n 54 above) 107.

Union (AU) and the Southern African Development Community (SADC) and both regional organisations have data privacy instruments. South Africa's data privacy regime has, nevertheless, been substantially influenced by the EU rather than the regional organisation which South Africa belongs. [83] All in all, it can be safely argued that both Canada and South Africa fairly represent the major approaches to data privacy regulation and make for an interesting discussion from a comparative perspective.

1.6. Clarification of terminologies

Three terms are central to this research study, viz - 'data privacy', 'personal information' and 'lesson-drawing'. It is important, therefore, to clarify their meanings within the context of this thesis, so as to further delimit the scope of this research.

1.6.1. Data privacy (protection)

Unlike privacy, the term 'data privacy' is, arguably, not fraught with definitional difficulties.[84] This is without prejudice to the generally acknowledged problems associated with the conceptualisation of legal terminologies.[85] What, however, brings about conceptual difficulties is the appropriate terminology to describe the *sui generis* protection

---

83 Even though the crucial role of the EU in the emergence and development of data privacy law (especially in the human rights perspective) has been frequently acknowledged, this research does not focus on that jurisdiction for a number of reasons. Firstly, it is thought that the EU regime (represented by the EU Directive and draft EU Regulation) is supra-natural in nature and may, arguably, not be an ideal model from which to obtain insights especially with regard to specifics in a data privacy regime. This is because, in many instances, provisions are coached in a fairly broad manner allowing member states to transpose them in a way that fits their local circumstances. Secondly, the EU regime is currently undergoing some reforms which may take some time, and it is still largely uncertain when the reforms will materialise. Thus, there are still some uncertainties on data privacy in the EU. This study, nevertheless, notes some of the proposed reforms for the purpose of lesson drawing. On another front, quite a number of scholars (especially African) tend to discuss data privacy with primary reference to the EU without considering the salient lessons that can be gained from other jurisdictions. In this regard, if we keep arguing that scholarship on data privacy in Africa is developing at a very slow pace, scholars on data privacy are not really helping the situation if they merely keep focusing their research on the EU (or making comparisons with the EU) without giving some consideration to African data privacy regimes. It must be stated, nonetheless, that, although this research does not focus on the EU, some insights were still obtained from the jurisdiction in a comparative perspective.

84 Several authors have acknowledged the difficulties in defining privacy. For examples, Finn notes that 'privacy has proved notoriously difficult to define.' R Finn *et al* 'seven types of privacy' in S Gutwirth *et al* (eds) *European data protection: Coming of age* (2013) 6. On the other hand, Tzanou, writing on data protection, argues that 'legal scholars writing on data protection do not seem to find it hard to describe the main essence of data protection laws'. Tzanou (n 35 above) 88. The definition of privacy is outside the scope of this work. For an in-depth discussion, however, see Fuster (n 18 above)22.

85 N Tobi *Sources of Nigerian law* (1996) 103.

of personal information.[86] While some scholars prefer to use the term 'privacy' or 'information privacy', others will use the term 'data protection'. These differences are a reflection of the jurisdiction which the discussion focuses on.[87] A term recently increasingly being used is 'data privacy'.[88] Although no recent data privacy instrument has adopted the term, it seems that 'data privacy' is the current preferred term as shown in the recent literature of renowned scholars, like Kuner,[89] Bygrave,[90] Greenleaf,[91] Makulilo.[92] Bygrave explains his preference for data privacy over privacy or data protection. He argues that it reduces the over-inclusion problem associated with the term 'privacy',[93] and it communicates better the central interests at stake.[94] The term 'data privacy', furthermore, 'provides a bridge for synthesising European and non-European legal discourses'.[95] Because of Bygrave's logical and convincing argument, and other reasons that will emerge later, this thesis adopts the term 'data privacy' rather than '(information) privacy' or 'data protection'.[96]

---

86 Indeed Bygrave observes that '[t]he issue of nomenclature might be dismissed as trivial since it primarily relates to "packaging". Yet the packaging sends important signals about the law's remit, particularly to newcomers.' Bygrave (n 64 above) 23.

87 'Privacy' is the preferred term used in the US and associate countries like Canada. The rationale for the preference of the term privacy is the theory that data privacy is merely a subcategory of privacy. This view is held based on the definition of privacy by Alan Westin whose definition of privacy is that '[p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.' A Westin *Privacy and freedom* (1967) 7. On the other hand, the preferred terminology in European discussion is 'data protection' which is a German coinage *Datenschuz.* According to Bygrave, *Datenschuz* is, in turn, derived from the notions of *Datensicherung* and *Datensicherheit* meaning 'data security'. LA Bygrave *Data protection law: Approaching its rationale, logic and limits* (2002) 22. For more in-depth discussion of the politics of the terminology, see Bygrave (n 62 above) 23-29. See also AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) *International Data Privacy Law* 164-167.

88 Zalnieriute (n 9 above) 105.

89 The scholar uses data privacy in C Kuner *Transborder data flow and data privacy law* (2013) although data protection was used in older works like Kuner (n 5 above). Kuner appears to be inconsistent with his use of the terminology as he has adopted data privacy in previous works too. See Kuner (n 10 above).

90 The scholar uses data privacy in Bygrave (n 64 above) although data protection was used in older works like Bygrave (n 87 above).

91 Unlike other scholars, Greenleaf has consistently used 'privacy' in his works. He, however, used data privacy in a recent book. See Greenleaf (n 44 above).

92 Makulilo uses 'privacy and data protection' or 'data protection' in older works but he uses data privacy in current works, such as Makulilo (n 40 above). See also the title of a journal *International data privacy law* published by Oxford University Press.

93 The over inclusion problem of the term 'privacy' has various aspects which are *stricto sensu* outside the scope of data privacy. Bygrave (n 64 above) 29.

94 Bygrave (n 64 above) 29.

95 Bygrave (n 64 above) 29.

96 Except where explicitly stated otherwise. Moreover, relying on the view of some writers, Bygrave canvassed an insightful and logical argument against the term 'data protection'. I will reproduce the comments of the learned scholar here. He states: "The term 'data protection' is problematic on multiple counts. It fails to indicate expressly the central interests served by the norms to which it is meant to

The crucial question then is, 'what is data privacy (protection)?' De Hert and Gutwirth contend that data privacy, though impossible to summarise in few words, is a catch-all term for a series of ideas regarding the processing of personal data.[97] They further argue that governments use these series of ideas to reconcile fundamental, but conflicting objectives, such as privacy, free flow of information, and the need for government surveillance.[98] This definition, it is submitted, is vague as it does not tell us what threats data privacy seeks to prevent and who it protects. The definition of scholars like Neethling *et al*[99] and Roos[100] take care of these apparent lapses. The scholars define data privacy (protection) as the protection of persons from harm resulting from the processing of their personal information by data controllers. In the same vein, Bygrave defines data privacy in terms of a law 'aimed primarily at safeguarding certain interests and rights of individuals in their role as data subjects - that is, when data about them is processed by others. The interests and rights are usually expressed in terms of privacy, and sometimes in terms of autonomy or integrity.'[101] In essence, data privacy basically seeks to protect individuals (and in some cases, corporate persons) from risks resulting from the processing of their personal information. The *sui generis* nature of data privacy can also be discerned from Bygrave's definition which shows that data privacy serves a multiplicity of interest beyond privacy interests.[102] De Hert and Gutwirth make a similar observation when they point out that data privacy explicitly protects values that are not at the core of privacy.[103] A data privacy law within the context of this thesis, therefore, is a law that contains all or most of

---

apply. It is misleading insofar as it 'suggests that *the data* are being protected, instead of *the individual* whose data are involved'. It has an 'unnecessary technical and esoteric air'. And it has connoted in some circles concern for data security and for the protection of intellectual property rights." Bygrave (n 62 above) 28. See also H Burkert 'Privacy – data protection: A German/European perspective in C Engel & KH Keller (eds) *Governance of global networks in the light of differing local value* (2000) 46 who suggest that the term 'data protection' is misleading since the subject of protection is not the data but the individual's human right to privacy.

97 P De Hert & S Gutwirth 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalization in action' in S Gutwirth *et al* (eds) *Reinventing data protection?* (2009) 3.

98 De Hert & Gutwirth (n 97 above) 3.

99 Neethling (n 36 above) 267.

100 Roos (n 65 above) 313.

101 Bygrave (n 64 above) 1. See also Kuner's definition that 'data protection law seeks to give rights to individuals in how data identifying them or pertaining to them are processed, and to subject such processing to a defined set of safeguards.' Kuner (n 79 above) 308.

102 These issues will be discussed further in the next chapter. Suffice it to mention at this point that Bygrave contends that 'in some respects, data privacy canvasses more than what are typically regarded as privacy concerns.' Bygrave (n 64 above) 3.

103 Such as the requirement of fair processing, consent, legitimacy and non-discrimination. See De Hert & Gutwirth (n 97 above) 9. See also S Gutwirth & M Hilderbrandt 'Some caveats on profiling' in S Gutwirth *et al* (eds) *Data protection in a profiled world* (2010) 36.

the FIPs which regulate personal information processing.[104] The law operates *ex ante* without necessarily waiting for an infringement to occur.[105]

There are, arguably, no settled theories explaining data privacy, unlike privacy, because it is still a developing area of law.[106] Tzanou, however, in a very insightful study, identifies two theories explaining the nature of data privacy which is essentially captured in the above paragraph.[107] The first theory, 'the separatist model', stresses the 'added-value' of the right to data privacy.[108] Tzanou sees this theory as the 'most comprehensive theory of data protection elaborated so far' in the literature.[109] The second theory is 'instrumentalist model' which rejects the arguments of the 'separatist model' and contends that data privacy (and privacy) merely has an intermediate value as it serves as a tool for the fulfilment of other human rights like dignity and personality.[110] This thesis basically adopts both theories as data privacy has an 'added-value' beyond the right to privacy because of the need to foster other values which were, *stricto sensu*, outside the scope of privacy.

1.6.2. Personal data/information

An understanding of what constitutes 'personal data' or information[111] is critical for an investigation on data privacy as the existence of personal data is a jurisdictional trigger to

104 Bygrave (n 64 above) 2.

105 In this respect, some commentators observe that unlike mechanisms that protect personality, which are mostly used retroactively (*ex post*), data protection tries predominantly to guarantee the protection in advance (*ex ante*) by considering the processing of data as privacy infringing "by default" and therefore making processors adhere to data quality principles. A Tamò & D George 'Oblivion, erasure and forgetting in the digital age' (2014) 2 *Journal of Intellectual Property, Information Technology & E-commerce* 72.

106 See Fuster (n 18 above) 4, arguing that literature on the right of data privacy is limited because the right is still relatively novel. Makulilo, in his doctoral thesis, examined quite a number of privacy theories. It is the view of this researcher nevertheless, that the theories he discussed explain privacy to a larger extent rather than data privacy. This is with the exception of the information control theory. See Makulilo (n 12 above) 66-105.

107 Tzanou (n 35 above) 92-96.

108 De Hert & Gutwirth are the main proponents of this theory. See De Hert & Gutwirth (n 97 above)

109 Tzanou (n 35 above) 93.

110 The main proponent of this theory is A Rouvroy & Y Poullet 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy' in S Gutwirth *et al* (eds) *Reinventing data protection* (2009) 45-76.

111 According to Roos, data are 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 (n 65 above) 313. Both information and data are, thus, used interchangeably in this thesis as Bygrave observes 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 (n 87 above) 20.

data privacy laws.[112] Schwartz and Solove note that 'personal data' is a 'central concept in [data] privacy regulation around the world.'[113] Indeed, '[n]ot all types of data fall within its [data privacy] ambit.'[114] Bygrave observes that, '[d]ata privacy law regulates all or most stages in the processing *of certain kind of data.*'[115] A common misconception with respect to the notion of personal information under data privacy law is that it is information which is private, secret or confidential. This misconception seems to be because of the use of the word 'personal', being interpreted to mean 'private'. Arguably, this conception also appears to be the traditional understanding that prevailed in data privacy texts. Wacks, for example, thus, defines personal information as 'those facts, communications, or opinions which relate to the individual and which it would be reasonable *to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use or circulation.*'[116] The current meaning of personal information based on all international data privacy codes is that it is information which relates to an individual.[117] From this perspective, information need not be private or secret for it to fall within the scope of data privacy law.[118] It is sufficient if such information merely identifies (or is capable of identifying) an individual. Based on this understanding, Lynskey consistently argues that data privacy is wider than privacy as it 'provides individuals with more rights over more types of data than the right to privacy.'[119] In the same vein, Solove argues that 'information about an individual […] is often not secret.'[120] Van der Sloot also acknowledges the fact that processing under data privacy laws (the EU) 'often does not handle private or sensitive data but public and non-sensitive data such as car ownership, postal codes, number of children, etc.'[121]

---

112 PM Schwartz & DJ Solove 'Reconciling personal information in the United States and European Union' (2014) 102 *California Law Review* 879.

113 Schwartz & Solove (n 112 above) 878.

114 Bygrave (n 64 above) 1.

115 Bygrave (n 64 above) 1. (Emphasis supplied).

116 R Wacks *Personal information privacy and the law* (1989) 26. [Emphasis supplied].

117 See CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, art 2; EU Directive, art 2.

118 Indeed, the Court of First Instance of the European Community pointed out that not all personal information is private as 'not all personal data are necessarily capable of undermining the private life of the person concerned.' See *Bavarian Lager* case, CASE T-194/04 Judgment of 8 November 2007, paras 118-119.

119 O Lynskey 'Deconstructing data protection: The 'added value' of a right to data protection in the EU legal order' (2014) 63(3) *International and Comparative Law Quarterly* 569.

120 Solove (n 42 above) 43.

121 B Van der Sloot 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 307.

In essence, this thesis consistently pursues the theory that personal information is broader than private information, but may, in many circumstances, include private information. It also claims that data privacy, even though, normatively based on the right to privacy, has an 'added-value' beyond the scope of the right to privacy. The issues will be elaborated upon in the next chapter.

1.6.3. Lesson-drawing

As earlier mentioned, this study basically draws lessons from other jurisdictions toward realising effective data privacy protection in Nigeria. It is therefore pertinent to understand the meaning of the term 'lesson-drawing' within the context of this thesis. Colin Bennett provides some insights into what the 'art of lesson-drawing' involves in legal and policy formulations. He states that:

> "Lesson drawing" is a more specific concept than "learning" or "emulation." It denotes a more conscious and deliberate search for possible solutions across time and space, by policy-makers acting either individually or collectively […] It might be defined as the process of deriving practical conclusions about the effectiveness of a program elsewhere and about its transferability to one's own political system.[122].

With regard to data privacy specifically, the South African Law Reform Commission (SALRC) rightly observed that while it is important to draw-lessons from the experiences of other countries, it is dangerous to translate the experiences of other countries directly into one's own law.[123] This thesis, therefore, put all these facts into consideration in examining the Canadian and South African data privacy regime.

1.7. Literature review

Because of the significance of data privacy as a contemporary human right, it has attracted a great deal of attention from scholars and policymakers worldwide. Nonetheless, Fuster, as of late 2014, contends that data privacy law is still relatively novel and, therefore, the literature on it is limited.[124] While her contention may be a proper description in relation to scholarly works in Africa, which Makulilo notes 'remained scant, fragmented and [have] continued to grow at snail's pace', it may be difficult to agree with her with regard to

---

122 CJ Bennett 'The formation of a Canadian privacy policy: the art and craft of lesson-drawing' (1990) 33 *Canadian Public Administration* 553-554.

123 SALRC (n 26 above) 615.

124 Fuster (n 18 above) 3.

literature in other parts of the world.[125] Scholarly works on data privacy in Nigeria is even scantier than some other jurisdictions in Africa like South Africa. As noted earlier, this study investigates how the protection of data privacy can be effectively realised in Nigeria based on lessons learnt from selected jurisdictions. It is for this reason that this review considers only existing works in Nigeria.

Literature on data privacy in Nigeria can largely be categorised based on the main issues considered. Some of the works, however, fall into more than one category. The first category consists of literature which identifies several data privacy challenges in Nigeria. In this respect, quite a number of commentators have devoted considerable attention to articulating the data privacy problem in Nigeria, especially in the light of recent advances in ICTs. Adeniyi recently advocated the need for data privacy law in Nigeria.[126] His contention is based on an analysis of the data privacy challenge which resulted from the recent SIM card registration directive of the government. He argues that '[a]s laudable as the goal of the directive may seem, the registration of [a] SIM card poses [an] inherent danger to the security of Nigerians.'[127] Izuogu also carried out a similar but more detailed study of the government policy.[128] Both scholars conclude that the solution to the personal information proliferation would be the adoption of a law in line with the EU Directive without anything more. Adelola *et al* discuss the data privacy challenge resulting from the emergence of e-commerce and the proliferation of the internet.[129] Their discussion is quite brief and devoted rather too much space to an analysis of the legal framework of other jurisdictions. Jemilohun, in an article on legislating for cyberspace, also briefly raised concerns on biometric information collection by the Independent National Electoral Commission (INEC) during the last general election.[130] A country report by the Electronic Privacy Information Centre (EPIC) provides details on data privacy challenges that arise

125 Makulilo (n 87 above) 163.

126 AS Adeniyi 'The need for data protection law in Nigeria' https://adeadeniyi.wordpress.com/2012/07/18/the-need-for-data-protection-law-in-nigeria-2/ (accessed 1 November 2015).

127 Adeniyi (n 126 above).

128 CE Izuogu 'Data protection and other implications of the ongoing SIM card registration process' http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665 (accessed 1 November 2015).

129 T Adelola *et al* 'Privacy and data protection in e-commerce in developing nations: Evaluation of different data protection approaches (2015) 6(1&2) *International Journal of Digital Society* 950.

130 BO Jemilohun & TI Akomolede 'Legislating for cyberspace: Challenges for the Nigeria legislature' (2015) 38 *Journal of Law, Policy and Globalization* 134.

from a comprehensive national identity database in Nigeria.[131] Yusuff considers the impact of the growing use of CCTV cameras in public places in Nigeria.[132] His robust discussion, however, does not devote much space to the Nigerian situation. A publication by Freedom House presents facts on systematic government surveillance of the activities of people on the internet. [133] All the above works are narrow as they consider only specific challenges resulting from the proliferation of ICTs in Nigeria. A recent article by this researcher brings together most of these issues in a concise form and identifies other overlooked threats to data privacy, such as the data processing activities of credit bureaus in Nigeria.[134] This thesis takes these discussions further by elaborating on most of these issues based on an analysis of recent data processing activities.

The second category of literature in Nigeria evaluates the extant legal framework on data privacy protection. Most scholarship falls into this category. Two scholars consider data privacy protection elaborately in their doctoral dissertations.[135] A cursory look at these works shows that data privacy is currently protected via the Constitution, common law, sectoral law and soft laws (regulations and guidelines). Allotey, in discussing transborder data flow (TBDF), evaluates the privacy and data privacy regime.[136] He concludes that the extant legal framework is insufficient to enable Nigeria to benefit from the global network economy. He identifies several reasons for the paucity of case law on privacy (and data privacy).[137] Laosebikan also carries out a similar study, with, however, a special focus on internet cafés.[138] She concludes, like Allotey, that '[i]n Nigeria, while protection is provided for the right to privacy in the Constitution and under certain statutes, there is very little constitutional protection for data.'[139] Other works, like those of Nwauche,[140]

---

131 EPIC 'Privacy and human rights report 2006 of the Federal Republic of Nigeria' available at http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Federal-3.html#Heading9594 (accessed 1 November 2015).

132 AOA Yusuff 'Legal issues and challenges in the use of security (CCTV) cameras in public places: Lessons from Canada' (2011) 23 *Sri Lanka Journal of International Law* 33.

133 Freedom House 'Nigeria' 2013 https://freedomhouse.org/report/freedom-net/2013/nigeria (accessed 1 November 2015).

134 Abdulrauf (n 41 above) 81-85.

135 FO Laosebikan 'Privacy and technological development: A comparative analysis of South African and Nigerian Privacy and Data Protection Laws with particular reference to the protection of privacy and data in internet cafes and suggestions for appropriate Legislation in Nigeria' unpublished Ph.D. thesis, University of Kwazulu-Natal, 2007; AKE Allotey 'Data protection and transborder data flows: Implication for Nigeria's integration into the global network economy' unpublished LLD thesis, University of South-Africa, 2014.

136 See chapter 4, Allotey (n 135 above).

137 Allotey (n 135 above)188.

138 Laoesbikan (n 135 above).

139 Allotey (n 135 above)431.

Kusamotu,[141] Jemilohun,[142] Akinsuyi,[143] and Puddephatt *et al*[144] also briefly examine the extant legal regime and reach conclusions similar to those of Allotey and Laosebikan. A closer look at all these works shows that the discussions on privacy and data privacy are conflated, thereby suppressing the added-value of a right to data privacy. A more lucid example of this fact is the thesis by Salami, which appears to be skewed in favour of data privacy being solely for the purpose of protecting the confidentiality of personal information.[145] An article by this researcher points out that there is a total neglect of data privacy in Nigeria based on an analysis of the present data privacy regime *vis-à-vis* the current processing activities.[146] In this article, the point was made that a lack of recognition of the subtle differences between data privacy and privacy is one of the reasons for the neglect of data privacy in Nigeria. This thesis expands on this argument by focusing narrowly on data privacy alone, thereby bringing out its added-value in this information society.

Arguably, most current works are silent on the human rights dimension of data privacy. This issue leads to the third category of literature which discusses the need for data privacy because of the economic benefits that are likely to accrue to Nigeria especially from the standpoint of trade with the EU. In this category comes the works of Allotey,[147] Kusamotu[148] and Akinsuyi.[149] Allotey's research focuses on data privacy as an international trade issue where a robust discussion is carried out on the need for Nigeria to integrate into the global network economy.[150] The present study is different in that it focuses on the human rights value of data privacy. This is not to say, however, that the

---

140 ES Nwauche 'The right to privacy in Nigeria' (2007) 1(1) *Review of Nigerian Law and Practice* 64-90.

141 A Kusamotu 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by Article 25 of European Union Directive 95/46' (2007) 16(2) *Information & Communications Technology Law* 149-159.

142 Jemilohun (n 54 above). See also BO Jemilohun & TI Akomolede 'Regulations or legislations for data protection in Nigeria? A call for a clear legislative framework' (2015) 3(4) *Global Journal of Politics and Law Research* 1-16.

143 FF Akinsuyi 'Data protection legislation for Nigeria: The time is now!' http://www.datalaws.com/pdf/article02.pdf (accessed 1 November 2015).

144 T Mendel *et al Global survey on internet privacy and freedom of expression* (2012) 90.

145 OO 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' unpublished LLM thesis, Dalhousie University, 2015.

146 Abdulrauf (n 41 above) 68-95.

147 Allotey (n 135 above).

148 Kusamotu (n 141 above).

149 FF Akinsuyi 'Data protection and privacy laws in Nigeria: A trillion dollar opportunity!!' http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2598603 (accessed 1 November 2015).

150 Allotey (n 135 above).

economic benefits are not important; far from it. The argument canvassed herein is that human rights should always be prioritised.

One issue that seems to be absent in discussions on data privacy in Nigeria is the extent of the influence of regional and sub-regional instruments in realising data privacy in Nigeria. With the exception of Allotey,[151] most of the available literature seem to overlook the two regional data privacy codes that have a direct effect on Nigeria. This study fills this gap by opening up a grey area for further research on the influence of regional data privacy instruments in stimulating respect for the data privacy right by governments and private entities. This thesis, therefore, pushes Allotey's research forward by discussing not only the Economic Community of West African States (ECOWAS) framework, but also the recent AU Convention on Cyber-Security and Personal Data Protection and the extent of their influence on data privacy protection in Nigeria.

Not so much scholarly attention has been devoted to a comprehensive analysis of the proposed data privacy laws in Nigeria and the issues arising from them. Indeed, quite a number of scholars have listed Nigeria among the African countries with pending data privacy draft bills without further detail.[152] Two works which discuss the current draft bills also show the Nigerian problem when it comes to legislation. Makulilo analyses the Data Protection Bill of 2010 and argues that it contains 'too many surprises' because of its significant flaws.[153] Article 19, an NGO, undertakes a similar analysis.[154] Its analysis is, however, based on another draft bill, the Personal Information and Data Protection Bill. Like Makulilo, Article 19 concludes that 'the bill is poorly drafted and confusing.'[155] Both Makulilo and Article 19 further point out that the Bills are inconsistent with the ECOWAS instrument on data privacy. This thesis advances the debate on the pending laws with a view to evaluating their viability should any of them be enacted.

The last category of literature discusses how data privacy can be realised in Nigeria. In this regard, Nwauche argues that the extant constitutional and common law regime is sufficient

151 Allotey (n 135 above) 298.
152 Greenleaf (n 66 above); Makulilo (n 40 above).
153 AB Makulilo 'Nigeria's Data Protection Bill: Too many surprises' (2012) 120 *Privacy Law and Business International Report* 26.
154 Article 19 'Nigeria Personal Information and Data Protection Bill' (2013) available at http://www.article19.org/resources.php/resource/3683/en/nigeria:-personal-information-and-data-protection-bill (accessed 1 November 2015).
155 Article 19 (n 154 above).

for the effective protection of data privacy.[156] Other scholars recommend that Nigeria should learn lessons from other jurisdictions. While Jemilohun[157] and Allotey,[158] on the one hand, contend that crucial lessons can be learnt from jurisdictions like the UK, Canada and India; the bulk of literature, on the other hand, suggests that a law quite similar to the EU Directive should be adopted obviously because of its global impact as acknowledged by many commentators. In this respect, Salami, argues that the EU model law is workable in Nigeria because South Africa has successfully adopted it.[159] Obviously, her discussion seems to be oblivious of the fact that, in the preparation of the POPIA, considerable attention and space was devoted to evaluating other legal regimes beyond the EU as shown in the *travaux préparatoires*.[160] The present study engages in a deeper analysis of how data privacy can be realised and argues that other important issues beyond the mere copying of foreign data privacy law must be taken into consideration.

On the whole, this study is significant because of the necessity to update literature constantly in an area such as data privacy law which is in a constant state of flux. That apart, an overview of the above issues considered in the current literature highlights certain gaps which this thesis fills. In summary, firstly, there is no comprehensive study that specifically deals with data privacy independent of the 'traditional' right to privacy. Secondly, most of the available literature do not focus on the human rights perspective of data privacy, but is, rather, more concerned with its economic implications. Thirdly, many scholars merely advocate that a data privacy law in line with the EU Directive be adopted without an in-depth analysis of other salient issues involved. Most of the works, furthermore, do not carefully consider the contents of a data privacy law and how they can be used towards advancing the right of individuals.

1.8. Structure of the thesis

Chapter one sets the base for the study. It looks at the general background and states the primary problem that provoked this research. In addition, the chapter sets out the objectives of the study and the questions to be investigated. Chapter one finally contains

156 Nwauche (n 140 above).
157 Jemilohun (n 54 above) recommended UK, Canada and India.
158 Allotey (n 135 above) 359 recommended US, UK, Australia and South Africa.
159 Salami (n 145 above) 134. she contends that '[t]he argument is that if legislation based on the European model could work in South Africa, its potential for Nigeria must, at least, be explored.'
160 See generally SALRC (n 26 above).

the methodology, scope and limitation of the study, and a review of existing scholarship on the topic.

Chapter two contains a series of preliminary reflections on data privacy generally. Firstly, it discusses the emergence and development of data privacy law through national, international and regional instruments. Then, some reflection on the debate regarding data privacy as a contemporary human right is carried out. The nature of the relationship between data privacy and privacy is further discussed. The chapter also considers approaches to data privacy protection. In addition, chapter two examines other (non-legal) mechanisms in protecting data privacy. In concluding, this chapter evaluates the major arguments against the right to data privacy.

Based on the foundation laid in chapter two, chapter three evaluates the legal framework for data privacy protection in Nigeria. This chapter further expands on the main research problem of this study. It reflects on current major data privacy issues in Nigeria and analyses the extant legal regime for data privacy protection. The chapter also evaluates the major draft bills on data privacy in Nigeria. Furthermore, an analysis of regional and sub-regional data privacy instruments and the extent of their influence on data privacy protection in Nigeria are carried out. Finally, the chapter considers, in detail, the major impediments to effective data privacy protection in Nigeria.

Chapters four and five examine the legal framework for data privacy protection in Canada and South Africa respectively. Firstly, the chapters appraise the major data privacy issues in these countries and attempt to establish a *nexus* with what obtains in Nigeria to further justify the choice of the countries. Secondly, a detailed exposé of the conceptual basis and approach to data privacy in the countries is carried out. Based on this background, the chapters analyse the legal framework and institutional mechanisms for data privacy in both countries with the view to obtaining lessons for Nigeria. An analysis is also carried out on the extent of influence of international data privacy codes on the Canadian and South African data privacy regime. The chapters also discuss other minor issues like proposals for legislative reforms of the data privacy regime with particular reference to Canada.

Chapter six considers the prospects for improving the data privacy regime based on contemporary debate on particular focus areas. In this regard, the rights-based approach to data privacy protection which basically emerged from Europe is examined based on

current literature. Similarly, the feasibility of a rights-based data privacy regime in Nigeria is examined, based on a comparative study of particular aspects of the Canadian and South African data privacy regimes. In essence, this chapter puts some of the lessons obtained in the two previous chapters into proper human rights context.

Chapter seven summarises and concludes the study by putting together the lessons obtained from the previous chapters and making recommendations for the effective realisation of the right to data privacy in Nigeria.

Chapter two

The emergence and development of the *sui generis* right to data privacy

2.1. Introduction

> *Data protection is not only a fundamental right among others but the most expressive of the contemporary human condition. Recalling this at all times is not a vaniloquy, because any changes affecting data protection impact on the degree of democracy we all can experience.*[1]

The right to data privacy is, without a doubt, an important contemporary issue in this age of 'big data' and 'digital devices'. Its development has enjoyed a rapid pace within a relatively short period of time. Data privacy law has been discussed and deliberated upon in several fora.[2] These discussions and deliberations are continuous, which depicts its increasing significance. It also goes to show that new challenges to personal data arises all the time, hence national and international institutions must devise means to tackle emerging threats to data privacy. Personal data has with time become a powerful resource. It is described differently by various commentators to depict its importance in modern society. Personal data is said to be a 'commodity', a 'property' and a 'valuable commodity'.[3] In fact, it is depicted as the 'new oil' of the information and the digital

1 S Rodotà 'Data protection as a fundamental right' in S. Gutwirth *et al* (eds) *Reinventing data protection* (2009) 82.

2 These discussions are mainly in international and regional organisations such as the United Nations (UN), Council of Europe (CoE), Organization of Economic Cooperation and Development (OECD), World Trade Organization (WTO) and many more.

3 Lloyd further contends that personal information, apart from being a commodity in its own right, 'is the motor and fuel which drives the information society'. IJ Lloyd *Information technology law* (2014) 22.

society,[4] hence, it is increasingly being transferred across borders. The significance of personal data in international trade is also obvious and has been considered in global trade institutions like the World Trade Organisation (WTO).[5] The material value of personal data and its increasing utility in this era of globalisation is not without its consequences. It exposes individuals to threats of abuse or misuse, and may affect their fundamental rights and freedoms in a democratic society. Hence, dedicated mechanisms are put in place to enhance individuals' control over their personal data and to ensure that it is only processed in accordance with specified laid down rules. This is done by conferring certain rights on individuals.

This chapter considers the emergence and development of the right to data privacy and its legal protection, especially, under international law. In so doing, some important issues will be examined as a prelude to the discussions. Parts 2.2 and 2.3, therefore, discuss the significance of personal data in the digital society, as well as the challenges posed to personal data in such a society. The historical development of data privacy law will then be examined in some depth in part 2.4. This will be done in accordance with the different stages in the development of data privacy law and the right to data privacy.

An important issue that will be explored is whether data privacy can properly be classified as a human right. The issue, which will be examined in part 2.5, is necessary because of its controversial 'split personality'.[6] Part 2.5 is also necessary so as to show that data privacy law should not be a concern of Western countries only. Since developing countries like Nigeria have human beings as subjects, it goes without saying that their data privacy right ought to also be guaranteed and protected. It therefore suggests that they also have to take part in debates on data privacy protection. Besides, it has been declared that data privacy is

---

4 Meglena Kuvena speech delivered at roundtable on online data collection, targeting and profiling Brussels, 31 March 2009 available at http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (accessed 1 November 2015).

5 See JK Winn 'Technical standards as data protection regulation' in S Gutwirth *et al* (eds) *Reinventing data protection* (2009) 194. This researcher has, elsewhere, discussed the importance of personal information from the perspective of transborder data flow for developing countries. See LA Abdulrauf 'Regulating transborder flow of personal information for development in the G77+China' (2015) *Latin American Studies Report* (forthcoming).

6 Split personality in this context is the two main agenda of data privacy law which are the commercial and human rights agenda. Thus, data privacy law can be said to be established for the purpose of achieving two main objectives. O Lynskey 'From market-making tool to fundamental right: The role of the Court of Justice in data protection's identity crisis' in S Gutwirth *et al* (eds) *European data protection: Coming of age* (2013) 59.

a 'right of every person irrespective of his nationality or residence'.[7] Another issue this chapter considers is the relationship between the right to data privacy and the right to privacy. This has been a very contentious topic which borders on the development of data privacy law. Debates of this nature are important because of the complex relationship between both rights. A better understanding of the rudiments of data privacy law is therefore centred on this issue which will be considered in part 2.6. Furthermore, although the essential principles of data privacy law are largely the same across jurisdictions, the approaches to data privacy protection vary, particularly with regard to the actors who play significant roles in the enforcement and implementation of data privacy principles. The chapter, in part 2.7, discusses the various regulatory approaches with regard to data privacy protection.

The role of non-legal mechanisms in data privacy protection is noteworthy. Using Lessig's theory, this chapter, in part 2.8, analyses how certain non-legal mechanisms can be tailored towards effective realisation of the right to data privacy. The chapter, furthermore, in part 2.9 considers some of the arguments against a right to data privacy. Part 2.10 concludes the chapter with some reflections, a brief summary and insights into the next chapter.

2.2. The significance of personal data in the information society

In the present day information society, the use of personal data is generating a new wave of opportunities for economic and social value creation.[8] The seamless accumulation and use of personal data justifies its current immense significance. The explosion in the volume of personal data and its use for commercial purposes is said to be 'one of the most important and controversial issues in the fast evolving world of digital communication.'[9] It is therefore not surprising that the former European Consumer Commissioner, Meglena Kuvena, described personal data as 'the new oil of the internet and the new currency of the digital world.'[10] Similarly, personal data has been referred to as the 'hottest commodity on

---

7 The declaration was made at the 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 1 November 2015).

8 World Economic Forum (WEF) 'Personal data: The emergence of a new asset class' (2011). Available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed 1 November 2015).

9 Kuvena (n 4 above).

10 Kuvena (n 4 above).

the market today - truly more valuable than gold'.[11] It 'will emerge as a new asset class touching all aspects of society'.[12] Consequently, this part of the chapter gives a brief overview of the significance of personal data in the information society.

Personal data is needed for a wide range of activities which include demographic, medical, planning and research and for commercial purposes. It is required in various sectors and by various entities. Personal information is primarily accumulated and used by the government and private entities, that is, public and private data controllers.[13] The relevance of personal data to both private and public entities is obvious and has been discussed on several occasions. What is less obvious, and rarely discussed, is the importance of personal data to individuals. All of these raise numerous legal issues regarding data privacy protection.

2.2.1. Public sector

Public entities, which consist of the state and its multiple agencies, need citizens' personal information for various purposes.[14] The act of governance or administration of the people is heavily dependent on the degree of knowledge the government has about its subjects. The only way in which the state can be informed about its subjects is through their personal information; that is, data that relates to its subjects or identifies them. This is to ensure delivery of a wide range of services such as education, welfare, health, and law enforcement. Many governments have launched e-government initiatives to improve communication amongst different agencies and to ensure that critical public services are delivered efficiently.[15] Personal data of individuals is important for the planning and budgeting functions of the state. Furthermore, it is needed for statistical and demographic purposes. The act of carrying out a census by the government is heavily dependent on

11 T Craig & ME Ludloff *Privacy and big data* (2011) 7.
12 WEF (n 8 above).
13 Thus, some authors, referring to personal data as a symbolism of ourselves, stated that '[w]e are the asset that every company, industry, non-profit, and government wants.' Craig & Ludloff (n 11 above) Back cover page.
14 Indeed, a commentator notes that '[i]ncreasingly governments are collecting data of their citizens under various administrative laws. These include registrations for cars, residency, taxation as well as financial information, marital status and electricity and water use. The information enables the government agencies to carry out their task more efficiently and increase service levels. However, with the collection of more and more data the risk increases as to its effect on the [data] privacy of an individual when combined with other data or disclosed to the public under a freedom of information request. See RH Weber 'The digital future -A challenge for privacy?' (2015) 31(2) *Computer Law & Security Review* 238.
15 WEF (n 8 above) 7.

collecting personal data of its citizens. Personal data is essential to the state for the purpose of renewal of the machinery of government through elections. The process of electronic voting (e-voting) can only be carried out when voters are identified by already accumulated biometric data.

The accumulation and use of personal data by the government is not a recent phenomenon. In fact, it is one of the reasons for the adoption of the first generation of data privacy laws.[16] The large databases owned and maintained by governments generated concern amongst privacy advocates and the citizens, since personal information were being used for purposes other than that for which the information was initially collected.[17] Databases of governments were also being hacked and unauthorised access was gained to personal data by unscrupulous persons for nefarious purposes. These breaches in security were largely due to poor data management practices. The concerns generated by the accumulation and use of personal data by the government led to the adoption of legislation holding the government accountable for data breaches.[18]

More recently, the collection of personal data by the state is taking place mainly for security and law enforcement purposes. With the increase in criminal activities brought about by the proliferation of new technologies, many governments increased their surveillance programmes and expanded their data collection practices. The spate of terrorism activities, especially since the 9/11 attacks in the United States,[19] results in governments wanting to know more about individuals. Access to the personal information of individuals is of course crucial in this respect. The government, with the necessary legal backing can obtain personal data from any source. In some cases, government officials have requested or subpoenaed Internet Service Providers (ISPs) to provide information about an internet user who is suspected of a criminal act.[20] In other cases, opposition

---

16 The first generation data privacy laws are the earliest set of data privacy legislation passed in the 1970s when data privacy emerged. This generation of laws were the data privacy laws of Germany, Sweden, USA, Canada, France etc. More on this will be discussed in part 2.4.1 below.

17 L Stefanick *Controlling knowledge: Freedom of information and privacy in a networked world* (2011) 43.

18 The increase in the processing of personal data by the government and the concerns that came with it is the reason why comprehensive legislation on data privacy only exists in the public sector in countries like the US. Canada, Australia and New Zealand also have a separate data privacy law regulating the public sector which was subsequently followed by legislation for the private sector.

19 IJ Lloyd *Information technology law* (2011)17-18.

20 DD Hirsch 'The law and policy of online privacy: Regulation, self-regulation or co-regulation?' (2011) 34 *Seattle University Law Review* 451.

members were unlawfully monitored without the necessary legal authorisation, such as warrants, which is in violation of their human right.[21]

Despite the importance of personal information to the government and its numerous institutions, it is being tasked with the difficult responsibility of ensuring that this information is adequately protected from the government itself, as well as private entities. This means that the government has to strike a delicate balance between protecting citizens' personal data on the one hand, and performing government functions such as fostering economic growth and promoting safety and public well-being on the other hand.

2.2.2. Private sector

In recent times, personal information has become vital in the private sector. [22] This is as a result of its commercialisation, since trading in information has now become a huge profit making venture.[23] The significance of personal data to private entities is shown by the fact that it is referred to as a raw material, like labour and capital.[24] Actors in the private sector need to know more about their consumers in order to improve their services.[25] They also need to promote their businesses to increase profits and turnover. Businesses need consumers' personal information regarding their choice and preferences for the purpose of targeted advertising and direct marketing. Personal data is also very important in the banking sector as banks also need to have customers' details to facilitate their transactions. Personal data is equally significant for insurance businesses as the very act of insurance is in itself, dependent on the concept of 'full disclosure' of personal information. In the employment field, employers need information about their (prospective) employees in order to make a decision about employing someone. The credit industry also needs information on customers so as to make informed decisions about lending out money.

---

21 Hirsch (n 20 above) 451.

22 WEF (n 8 above) 8. Indeed, Van der Sloot speaks of banalization of data processing which means 'data processing has generally moved from the public sector to the private sector and from large organizations to private individuals'. See B Van der Sloot 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 322.

23 Hirsch (n 20 above) 439.

24 'Data and Information both in public and private sector has become the new raw material of the world economy. Just as in the past centuries iron, wood and coal were foundation upon which the economy was based, so nowadays it is data and information'. D Kasneci 'Data protection law: Recent developments' unpublished PhD thesis, *Università Delgi Studi Di Trieste*, 2008/2009 3.

25 MD Birnhack 'The EU Data Protection Directive: An engine of a global regime' (2008) 24(6) *Computer Law & Security Review* 510.

Recently, there has been a growth in dedicated business agencies that specialise in collecting personal information. Most business enterprises need individuals' personal data, but may not have the capacity to collect, analyse and store such data. Special institutions, like credit bureaus, with specialised machinery and expertise to collect personal information are therefore necessary. Personal data collected by credit bureaus are sold to other actors in the private sector for their use. These dedicated businesses, specialised in collecting personal data, have become very big commercial ventures in recent times and accumulated personal data is their main raw material.[26]

Websites and network advertisers are also principal users of personal information on the internet. Network advertisers, particularly, are responsible for the banner advertisements that users see when visiting a website.[27] They enter into contractual relationships with other website owners to supply individuals' personal data to them.[28] Apart from websites and network advertisers, there are other private data users like data brokers and secondary users.[29]

Actors in the private sector present a far greater challenge to data privacy than the government because unlike the government, businesses are not limited in the use to which they put personal data. Over time, personal data has in fact become more valuable for commercial purposes than any other purpose. Indeed, Lessig notes that:

> Everything you do on the Net produces data. That data is, in aggregate, extremely valuable, more valuable to commerce than to government. The government (in normal times) really cares only that you obey some select set of laws. But commerce is keen to figure out how you want to spend your money, and data does that. With massive amounts of data about what you do and what you say, it becomes increasingly possible to market to you in a direct and effective way.[30]

The above discussion also shows that personal information is not only valuable for private entities that use it for commercial purposes, but also for the individuals whose information is in question.

---

26 J Neethling *et al Neethling's law of personality* (2005) 268.
27 Hirsch (n 20 above) 447.
28 Hirsch (n 20 above) 447.
29 For more elaborate discourse on this issue, see Hirsch (n 20 above) 439-480.
30 L Lessig *Code 2.0* (2006) 216.

2.2.3. Individuals or data subjects

Personal data is important to the individuals to whom they relate, that is the data subjects. This importance is somewhat paradoxical. This is because data subjects are the main subject of data privacy laws and their interest in their personal data is what is being protected. The personal data of an individual is sometimes considered to be the data subject's property and the data subject has a general interest in it.[31] The data subject is bestowed with a right of informational self-determination. This grants him/her some level of control to determine the use to which his/her personal data may be put. Information relating to a data subject is also important in other respects. Personal information of an individual is often traded on the internet in exchange for free services delivered by various service providers, such as social network services, email providers and cloud services.[32] These service providers accumulate individuals' personal data that is given out on the internet and use them for the purposes of direct marketing and advertising. Most of the services rendered by these service providers cannot be enjoyed without the supply of personal data. Moreover, certain service providers may offer reduced fees because users' personal information is being traded by the service providers for extra income. This emphasises the importance of an individual's personal information to the individual himself/herself.[33]

In other cases, these advertisements carried out by the service providers could also be important to the individuals. Direct marketing is usually carried out based on targeted advertising which is specifically tailored to meet the needs of an individual based on knowledge of certain information about him/her.[34] Kasenci observes that '[t]he new possibilities for processing data easily and cheaply […] might benefit consumers and citizens who enjoy personalized services to be identified than to be treated as part of the mass.'[35]

---

31 N Purtova *Property rights in personal data: A European perspective* (2012) 57, 193. See also JM Victor 'The EU General Data Protection Regulation: Toward a property regime for protecting data Privacy' (2013) 123 *The Yale Law Journal* 513.

32 See generally P Bernal *Internet privacy rights: Right to protect autonomy* (2014). Lessig (n 30 above).

33 Allen discusses how easily people are willing to give out their personal information nowadays on the internet which she refers to as 'the great information privacy give-way'. She therefore argues for an ethical duty of individuals to protect their own personal information. AL Allen 'An ethical duty to protect one's own information privacy?' (2013) 64 *Alabama Law Review* 845-866.

34 L Bergkamp 'The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy' (2002) 18 *Computer Law & Security Report* 31, 37.

35 Kasneci (n 24 above) 3.

The above discussion gives an overview of the significance of personal information to various entities. It shows the importance of personal information in the Information Technology (IT) driven society and its economic value. Nevertheless, the risk associated with unregulated personal data processing far exceeds its economic and commercial value.[36] This is the reason why significant attention is being placed on personal data to ensure that it is adequately protected. Unfortunately, new ways to facilitate its exploitation are constantly being invented.

2.3. The nature of the challenges to data privacy in the information society

The importance of personal data in the information society has made the innovation of new ways to facilitate its exploitation an increasingly attractive venture. These innovations have been made easy with the advances in technology, particularly, IT. IT has made it very easy to accumulate vast amounts of personal data with very little effort, for example by the mere click of a mouse.[37] IT has also facilitated the storage and transmission of this information. The profit-making incentive, in most cases, has brought about even more exploitation of personal data without regard to the interests of the individuals to whom the data relates. This is a huge challenge of the twenty-first century that has generated numerous legal issues.

Various technological innovations (new technologies) have brought about challenges to personal data and ultimately, to individuals' right to data privacy. These new technologies, otherwise called privacy-destroying technologies,[38] include computers and databases, the internet, surveillance technologies and cloud computing. This section examines some of these new technologies and how they constitute threats to personal data.

2.3.1. Computers and databases

The advent of computers and large databases was part of the driving forces behind the concerted action towards data privacy protection. The arrival of computers also served as

36 WEF (n 8 above) 8.

37 C Kuner 'An international legal framework for data protection: Issues and prospects' (2009) 25(4) *Computer Law & Security Review* 308.

38 The term 'privacy-destroying technologies' was used by Froomkin to refer to technologies that 'facilitate the acquisition of raw data and those that allow one to process and collate that data in interesting ways.' AM Froomkin 'The death of privacy?' (2000) 52 *Stanford Law Review* 1463.

an impetus for making information a valuable commodity.[39] The enhanced ability of computers to collect vast amount of information make them distinctive. They can also process and disseminate information collected with incredible speed.[40] Computers have the ability to store information for a very long period of time and such information can be easily recalled and analysed with little or no effort. Organisations therefore use computers to keep records for various purposes.[41] The rapid development of communication technology, connecting computers in networks, which enables the transmission of information via networks, further aided the ability of the computer to process personal data.[42] This is a challenge to data privacy. The computer also serves as a means to access other data privacy intrusive technologies that threatens individuals. For example, it is the main device through which collected personal data can be transmitted on the internet. Data collected through various surveillance technologies are also easily analysed with the aid of the computer.

The term 'database' is usually used with regard to computers.[43] It is defined as a '[l]arge body of information stored in a computer which can process it and from which particular bits of information can be retrieved as required.'[44] It operates like an electronic filing system. Governments and private entities maintain central data warehouses or databases (big data) that host large amount of personal data. These data warehouses are not physical warehouse that can be seen or perceived. They are usually imaginary and sometimes in a cloud which hosts volumes of data.[45] Central data warehousing brings about economies of scale. It also facilitates data processing and makes data management and use more efficient and effective.[46] With computers and the internet, databases are increasingly fed with personal data for storage purposes.

The issue with regard to databases is that in most cases, individuals do not know that their personal data is being hosted on a database. They, therefore, may not know who to hold accountable in case of harm resulting from a security breach of a database containing their personal information.

---

39 A Roos 'Data Protection' in D Van der Merwe *et al Information & communication technology law* (2008) 313.
40 Roos (n 39 above) 314.
41 Roos (n 39 above) 314.
42 Roos (n 39 above) 314.
43 Lloyd (n 19 above) 390.
44 Lloyd (n 19 above) 390 quoting Conscience Oxford Dictionary.
45 More elaborate discussion on cloud computing will be carried out in part 2.3.4 below.
46 Bergkamp (n 34 above) 32.

2.3.2. Internet

The internet is a very useful tool in the information society. It is a platform to carry out several tasks which make life easier for a user. Yet, by its nature, it is a powerful tool used in exploiting individuals' personal data.

The internet, despite its numerous benefits,[47] presents one of the greatest threats to data privacy. It has immense capacity to accumulate and store vast amount of personal data. Its ability to retrieve large amount of personal data from the most remote of sources makes it astonishing. Search engines in the internet have very powerful sorting and arrangement functions which provide the most accurate information about an individual without the need to laboriously go through large records or manual filing systems. Most discourse on the threats to individuals as a result of data processing is therefore largely focused on the internet. In fact, some countries enact data privacy laws which target electronic data collections aided by the internet only.[48]

The internet has given birth to commercial ventures with specific interest in personal data called 'data markets'.[49] These data markets are so organised that the various stages of data processing have been broken down whereby there are different entities that specialise in the collection, storage and use of personal data.[50] Websites and search engines are the major collectors of personal information on the internet. [51] Search engines, like google.com and ask.com, keep an extensive file of users' search requests.[52] More disturbing is the fact

---

47 Hirsch (n 20 above) 443. For an elaborate discussion on the nature of the internet, see A Murray *Information technology law: The law and the society* (2013) 15.

48 Eg, the Act on the Protection of Personal Information (Law No. 57 of 2003) (APPI) of Japan and the South African Electronic Communications and Transactions Act (ECTA) Act 25 of 2002. See R Moshell '…and then there was one: The outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection' (2004-2005) 37 *Texas Tech Law Review* 360-361.

49 'The internet has also given birth to [an] entirely new market: those dealing in the collection, organisation, and sale of personal information and those taking direct advantage of the internet as a commercial tool'. Moshell (n 48 above) 360.

50 Bergkamp states that '[i]n our information driven economy, there are many corporations that specialize in data mining, processing and management. Data collection, storage and processing often involve various entities.' (n 34 above) 32.

51 According to Hirsch 'search engines and website are major data collectors on the internet. The collection of users' information begins in search engine. They are able to link queries individuals make on the search engine both to the computer on which they are entered and to the user's individual identity. The search engines accumulate and store these queries for a long period of time. Beyond a search engine, websites also collect large amount of personal information regarding users.' (n 20 above) 444.

52 Eg, in 2006, a request was made by the US Justice Department to Google for data on how often and in what form people search for porn on the internet. This request was made because the Congress wanted to defend its latest regulation on pornography. Fortunately, Google, unlike other search engines like Yahoo and MSN refused the request. See Lessig (n 30 above) 204.

that these search requests could be easily linked to specific Internet Provider (IP) address and subsequently, to a person's user account. Thus, in the bowels of most search engines' databases is a massive list of all searches made by users, which could be easily used to identify them.[53] Websites designers have devised specialised methods to aid the collection of personal data. The most traditional being overt collection in which internet users are required to supply their personal data through online registrations, surveys, contests, applications and orders.[54] The user is deprived of access to a website or some of its functions if the requested personal data is not supplied.[55] Apart from the traditional overt collection, other more privacy intrusive methods are used to collect personal data on the internet. Cookies[56] are the most prevalent of these tools.[57] A cookie is an electronic text file that is placed on the hard drive of a computer by a website server when a user visits a website on the internet.[58] It enables a website server to develop a history of the communications between the user and the website visited.[59] The communications are based on places visited and the general activities of the user on a particular website. The server is in turn able to keep track of data of the user and recall the information on subsequent visits of the user.[60]

Clickstream is another recent tool increasingly being used and is considered a more sophisticated way of information collection.[61] Clickstreams collect information on sites visited by a user as well as how long he/she stays on each website.[62] Both tools (cookies

53 Lessig (n 30 above) 203-204.

54 AE Shimanek 'Do you want milk with those cookies: Complying with the Safe Harbor Privacy Principles' (2001) 26 *The Journal of Corporation Law* 460-461. See also Moshell (n 48 above) 362.

55 Shimanek (n 54 above) 460-461.

56 According to Roos, 'cookies are bits of data that are stored on an individual's computer when he or she visits a particular website. This enables the websites to keep a record of users of their site. Cookies may contain personalised information relating to the website that was visited, such as login codes, passwords, credit-card numbers or a list of shopping items.' Roos (n 39 above) 315. In 1994 cookies were introduced by Netscape as a protocol to make it possible for a web server to deposit a small bit of data on your computer when you accessed that server. That small bit of data, the cookie, makes it possible for the server to recognise you when you travelled to a different page. Lessig (n 30 above) 48.

57 MD Scott *Information technology law* (2012) 16-26. See also Shimanek (n 54 above) 459.

58 DJ Solove 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 53 *Stanford Law Review* 1411.

59 Scott (n 57 above) 16-26.

60 Scott (n 57 above) 16-26. The initial use of cookies was to make it easier for users to assess certain websites that requires authorisation as information supplies is already stored. When a user subsequently visits, he or she need not keep on supplying the same information.

61 Scott (n 51 above) 16-26. For more clickstream data and the challenges it poses to data privacy especially in the EU and US, see DB Garrie & R Wong 'Demystifying clickstream data: A European and US perspective' (2006) *Emory International Law Review* 563-589.

62 A clickstream is very similar to a cookie. However a clickstream differs from a cookie in that a cookie collects data of a user on a website but clickstream accumulates data of a user's activity on the internet

and clickstream) monitor and record users' activities on a website or the internet and are remotely transmitted to the data controller. Several concerns have been raised regarding the use of cookies and other devices to monitor users' habits on the internet.[63] This has led to efforts to prohibit its use.[64]

The information collected by means of these devices are used by other agents in the data market. These categories of persons specialise in the use of personal information for direct marketing and advertising purposes. Once personal data is collected, targeted advertising is carried out which are specifically directed to particular users based on their choices and preferences. This advertising method is very specific and based on analyses of aspects of a website visited. The information is also sold to other advertisers or direct marketers for their use. A common example of targeted advertising is Gmail, Google's emailing facility, which places adverts in email inboxes. These advertisements are in most cases based on the contents of the inboxes. This is a reason why most emailing services devise means to ensure that sufficient information is kept in our boxes.[65]

The internet has indeed generated legal issues regarding data privacy protection. Lessig summarises the challenges that the internet poses to individuals and the near impossibility to maintain anonymity on the internet. He states:

> That relative anonymity of the "old days" is now effectively gone. Everywhere you go on the Internet, the fact that IP address xxx.xxx.xxx.xxx went there is recorded. Everywhere you go where you've allowed a cookie to be deposited, the fact that the machine carrying that cookie went there is recorded—as well as all the data associated with that cookie. They know you from your mouse droppings. And as businesses and advertisers work more closely together, the span of data that can be aggregated about you becomes endless.[66]

---

as a whole and is not restricted to a particular website. Moshell (n 48 above) 362. Shimanek (n 54 above) 460.

63 Zimmerman R.K 'The way the "cookies" crumble: Internet privacy and data protection in the twenty-first century' (2000) 4 *Journal of Legislation and Public Policy*. 441.

64 Several lawsuits have also been brought regarding the use of cookies in different privacy laws in the US. See Scott (n 51 above) 16-26.

65 As Lessig explains, this is done by the absence of a facility that makes it easy to delete all the contents of our email boxes. In this manner, they ensure that emails are retained in our inboxes for a long period of time. Lessig (n 30 above) 205.

66 Lessig (n 30 above) 203.

2.3.3. Surveillance technologies

The proliferation of surveillance technologies that monitor people is a common feature in this digital era. Yusuff points out that we now 'live in a surveillance society where the creation, collection and processing of personal information by both public and private entities has become a ubiquitous phenomenon.'[67] Similarly, Lloyd notes that 'today, much is written and spoken about the increasing level of surveillance which permeates almost all aspects of our lives, with the consequential diminution of personal privacy'.[68] The security challenges today have made governments increase their investments in surveillance technologies that have the capabilities of capturing and analysing digital footprints.[69] This is in order to combat contemporary criminal activities such as terrorism.[70] This does not, however, mean that private entities are not involved in accumulating personal data using surveillance technologies. It is very rare today to enter a grocery store, bookshop, or bank without one form of surveillance device or another. Employers also monitor their employees using these technologies.

There are different types of surveillance which include physical surveillance, psychological surveillance and data surveillance.[71] The advances in digital technology have, however, blurred the strict categories.[72] While the utility of surveillance cannot be underestimated, most of the controversies about the proliferation of surveillance technologies are centred on the extent to which developments in IT facilitate the recording and retention of our everyday lives.[73] This includes details which hitherto could have gone unnoticed or could have been held for only a short period of time.[74] We unconsciously go about our daily lives without knowing that we are being monitored in one form or another.

There are various types of surveillance technologies. The most prevalent surveillance tool nowadays is the closed circuit television (CCTV).[75] Originally, video camera technology was a mild system of collection of personal data. This is because the product of their

---

67 AOA Yusuff 'Legal issues and challenges in the use of security (CCTV) cameras in public places: Lessons from Canada' (2011) 23 *Sri Lanka Journal of International Law* 34.
68 Lloyd (n 19 above) 3.
69 Craig and Ludloff (n 11 above) 7.
70 Craig and Ludloff (n 11 above) 7.
71 Identified by Alan Westin in his book *Information technology in a democracy*. Lloyd (n 3 above) 11.
72 Lloyd (n 3 above) 12.
73 Lloyd (n 19 above) 3.
74 Lloyd (n 19 above) 3.
75 Lloyd (n 19 above) 6.

monitoring was, to a larger extent, based on human interpretation.[76] Digital technology has now changed video surveillance. It is a tool of intelligence not just to record, but also to analyse data, independent of human inputs, based on specified rules of the programmer.[77]

Surveillance technologies have generated controversies in relation to the duties of the government to ensure the safety and security of the people. It is increasingly becoming difficult to strike a balance between the right to (data) privacy and the need to ensure the security of individuals, which is a very important function of government. Surveillance technologies raise issues such as whether the state should protect data privacy at the expense of securing the lives and properties of the people? This question has generated much debate as governments are now willing to do anything to ensure that the life and property of individuals are properly secured. In most cases, the government ignores other competing values such as privacy and data privacy.[78] Many countries are therefore increasing and improving their surveillance programmes for security purposes.[79]

Surveillance technologies are also usually combined with the internet to produce a very powerful tool of accumulation and storage of personal information. This is carried out using some of the internet monitoring devices discussed above and even more invasive devices such as Fin Fisher[80] which enables governments and private persons to be able to monitor users' activities on the internet.

---

76 Lessig (n 30 above) 207.

77 Lessig (n 30 above) 207; eg, the CCTV camera installed in major streets in London captures vehicles number plates and is able to link the number plate with the owner of the vehicle. Another example is the facial recognition cameras used for law enforcement purposes.

78 This can be seen in the attitude of the US government particularly after the 9/11 attack when surveillance activities of the government were drastically increased. This is also evident from the passing of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) which has been criticised because of its numerous infractions of fundamental rights and freedoms of the people, especially their right to privacy. See S Kashan 'The USA Patriot Act: Impacts on Freedom and Civil Liberties' (2009) 7 *ESSAI* 86-90.

79 The UK, for example, has more than 14 million surveillance cameras installed in different locations which mean approximately 1 for every 4 inhabitants. See Lloyd (n 3 above) 3. In the US, surveillance technologies are also heavily relied upon for law enforcement purposes. See Craig & Ludloff (n 11 above) 7. The use of surveillance technology is also growing in African countries. Recently, the Nigerian government signed an agreement with a Chinese telecommunication firm – ZTE - to install about 2000 solar powered CCTVs within the Federal Capital, Abuja and Lagos. Abuja and Lagos were selected to host the pilot projects aimed at closely monitoring and uncovering possible threats to public security through the CCTV cameras. 'Abuja: Where are the CCTV cameras?' http://www.thisdaylive.com/articles/abuja-where-are-the-cctv-cameras-/141195/ (accessed 1 November 2015).

80 This is a sophisticated spying software which can remotely monitor webmail and social networks in real time and collect encrypted data and communications of unsuspecting targets. It is mostly used by law enforcement agencies. It has been said that it is being abused by governments around the world. M

2.3.4. Cloud computing

Cloud computing is another ubiquitous computing concept that illustrates the challenge to protect personal information in the big data era. It is a new development of combining different services in a way that revolutionises computer and internet usage.[81] It has been said that the move to cloud computing demonstrates a cyclical progression in computing from centralised mainframes, to personal computers, and to personal computers tied together in clouds.[82] Cloud computing is the ability to access files, data, programs and third party services from a web browser through the internet and hosted by a third party provider.[83] In cloud computing, data and applications are centrally stored and can be remotely accessed through the internet by users anywhere in the world.[84] The striking feature of cloud computing is that existing and new computing applications are increasingly being performed in a 'cloud' - online - not on users' own hardware.[85] It therefore obliterates the problem of distance and location for the performance of certain task as users are connected via the cloud. This is one of the main advantages of cloud computing. Other advantages, according to Kong *et al* are: its cost effectiveness for the user as the cloud service provider owns and manages all the computing resources such as servers, software, storage and electricity (the user only needs to 'plug into the cloud'); reduction in waste of information systems and increased efficiency of data centres.[86] Cloud computing service is offered by entities such as Microsoft, IBM, AT& T and Amazon.[87]

Data privacy has been identified as one of the major legal concerns of the cloud computing model.[88] Cloud computing challenges data privacy protection due to the large amount of

---

Kelley 'This powerful spy software is being abused by governments around the world' http://www.businessinsider.com/countries-with-finfisher-spying-software-2013-5#ixzz31vYCYV4X (accessed 1 November 2015).

81 JP Sluijs *et al* 'Cloud computing in the EU policy sphere interoperability, Vertical integration and the internal market' (2012) 3 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 13.

82 RC Picker 'Competition and privacy in Web 2.0 and the cloud' (2008) 103 *North-Western University Law Review Colloquy* 1. See also G Zanfir 'The right to data portability in the context of the EU data protection reform' (2012) 3 *International Data Privacy Law* 151.

83 S Hodson 'What is cloud computing' cited in W Kim 'Cloud Computing: Today and Tomorrow' (2009) 8 *Journal of Object Technology* 65.

84 Slujis (n 81 above) 13.

85 Kim (n 83 above) 65.

86 J Kong *et al* 'Introduction to cloud computing and security issues' in ASY Cheung & RH Weber (eds) *Privacy and legal issues in cloud computing* (2015) 8-9.

87 Kim (n 83 above) 65.

88 P Balboni *et al* 'Cloud Computing. Benefits, Risks and Recommendations for information security' (2009) European Networks and Information Security Agency (ENISA)

personal data transferred and stored on a cloud by the user. In most cases, this information is automatically uploaded on a cloud account without the knowledge of the user.[89] Besides, users may not know who, where and how their information is being processed. With information, usually sensitive, out in the cloud, an individual loses control the information. Such information in the clouds has the capability of creating a digital personality of an individual in the digital world.[90] Cloud computing poses a much greater challenge for individuals, especially because of the recent sharp increase in the cases of breaches of clouds.[91]

The nature of a cloud computing service and the amount of personal data hosted makes it particularly attractive to hackers. Moreover, its shared and on-demand nature makes it volatile. There are numerous cases of security breaches of personal information on clouds by hackers. Recently, there was the case of security breach in apple's iCloud where hackers accessed celebrities' iCloud account and revealed some of their personal information such as nude pictures.[92] Most of the violated celebrities attested to the fact that pictures leaked have since been deleted.[93] This shows another dimension to the threat cloud computing poses as hackers have the capability to retrieve information from any source, even information already deleted. There are also cases of loss of data and data leakages associated with the cloud computing environment.[94]

---

http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/-fullReport (accessed 1 November 2015). See also Kong (n 86 above) 11

89 A user of an iPhone or iPad or mac usually has his/her personal information automatically backed up on an iCloud account created for him/her. See 'iCloud: iCloud storage and backup overview' http://support.apple.com/kb/ph12519 . Microsoft also has a similar facility for windows 7 and 8, called OneDrive. See 'Backup and restore' http://windows.microsoft.com/en-ZA/windows7/products/features/backup-and-restore (both cites accessed 1 November 2015).

90 Zanfir (n 82 above) 151.

91 To better illustrate the dimension of data breaches, the Cloud Security Alliance (CSA) identified 9 top threat of cloud computing in a document. InfoWorld.com 'The notorious nine: cloud computing top threats in 2013' https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf (accessed 1 November 2015).

92 Several celebrities were affected by this security breach of iCloud accounts. A Remling 'iCloud nude leaks: 26 celebrities affected in the nude photo scandal' http://www.ibtimes.com/icloud-nude-leaks-26-celebrities-affected-nude-photo-scandal-1692540 (accessed 1 November 2015). Apple automatically backs up information on an iPhone or iPad. This information is backed up on iCloud, Google and android. This shows that the information is available on more than one cloud. http://www.forbes.com/sites/markrogowsky/2014/09/03/the-celeb-hack-has-people-telling-you-to-turn-off-cloud-backup-ignore-them/ (accessed 1 November 2015).

93 Remling (n 92 above).

94 InfoWorld.com (n 91 above).

To enhance cloud integrity and data security, personal data stored in clouds are usually anonymised in a securely encrypted form called encryption.[95] The cloud provider will have no access to the decryption key.[96] This makes it factually impossible to identify a user using the information. Encryption too has its own downsides as a user can be indirectly identified through combining different sets of other pieces of information.[97] It is also possible, as demonstrated by computer scientists, to re-identify or de-anonymise data easily.[98] Moreover, de-anonymisation techniques are improving with time, especially with advances in technology. Hackers are constantly devising various means to decrypt and de-anonymise personal data on clouds. This has generated debates as anonymised data which cannot reasonably identify a data subject is not personal data and as such does not fall under the scope of data privacy laws.[99] However, recent times have exposed the inherent lapses of anonymisation of data. This is why some scholars have argued that the likelihood of identification should be the criteria for determining if a data can be categorised as personal and not necessarily the level of anonymisation.[100]

2.4. Historical development of the *sui generis* right to data privacy

The right to data privacy has enjoyed a very rapid growth within a relatively short period of time and is also in a constant state of flux.[101] It has evolved from a mere issue being considered by a few countries and international institutions to a topic that generates considerable debate worldwide. Despite its relative infancy, it has attracted significant scholarly attention.

---

95 Encryption involves turning ordinary information (or plaintext), such as letters or emails, into random strings of characters (or cipher text). Decryption is the reversal of this process. Both encryption and decryption require the use of specific algorithm and a key. D Rowland *et al Information technology law* (2011) 224.

96 Zanfir (n 82 above) 154; According to Hon *et al*, 'anonymized or pseudonymized data results from actions deliberately taken on personal data attempting to conceal or hide data subjects' identity'. See WK Hon *et al* 'The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing' (2011) 1(4) *International Data Privacy Law* 214.

97 See Zanfir (n 75 above) 154. See also Article 29 Working Party, 'Working Paper on the concept of personal data' (WP 136, 2007).

98 See Zanfir (n 75 above) 154.

99 Hon (n 89 above).

100 See Zanfir (n 75 above) 154.

101 M Albers 'Realizing the complexity of data protection' in S Gutwirth *et al* (eds) *Reloading data protection: Multidisciplinary insights and contemporary challenges* (2014) 221.

Several instruments at various levels have helped shape the different aspects of the right to data privacy. Paradoxically, most of these instruments are 'mere' soft laws.[102] This part of the chapter considers these instruments. It also presents an updated discussion on recent developments with regard to these instruments. The intention is not to consider all the available legal instruments on data privacy. Rather, instruments that have played the most significant role in the emergence and development of the right to data privacy will be discussed. A detailed analysis of the provisions of these instruments will also not be carried out as that is beyond the scope of this chapter.[103] The significant role played by Europe is particularly noted hence the bulk of this section will focus on the European initiatives.

2.4.1. Development of the right to data privacy through national instruments

The first step towards recognition and protection of the right to data privacy, separate from the right to privacy, began at the national level. The contributions of two countries towards the emergence of the right to data privacy are noteworthy. The first is Germany. The Federal State of Hesse passed the first data privacy law (referred to as a data protection law) in 1970.[104] The stated justification for the law was the growing opportunity to manipulate individual behaviour through sophisticated personal data processing.[105] Shortly thereafter, in 1971, a Bill was submitted for a Federal Data Protection Act.[106] The second country that played a significant role in the emergence of recognition of the right to data privacy was Sweden. In 1973, it enacted the first national data privacy law. Other countries like the US and Canada followed shortly with their Federal Privacy Acts in 1974 and 1975 respectively.

---

102 Soft laws are generally quasi-legal instruments which are non-binding such as guidelines, regulations and directives. This definition may, however, be overly simplistic. See generally GC Shaffer & MA Pollack 'Hard vs. soft law: Alternatives, compliments, and antagonists in international governance' (2010) 94 *Minnesota Law Review* 706. See also AT Guzman & TL Meyer 'International soft-law' (2010) 2(1) *Journal of Legal Analysis* 171.

103 Moreover, most of the basic principles and provisions of each of the instruments are largely contained in the individual data privacy laws which will be discussed in subsequent chapters of this work. For a detailed analysis of the provisions of these laws, see A Roos 'The law of data (privacy) protection: A comparative and theoretical study' unpublished LLD thesis, University of South Africa, 2003 149-242; Roos (n 34 above) 320-345; Bygrave (n 3 above) 31-82.

104 The US Fair Credit Reporting Act was also enacted in 1970, however, its contribution was not so significant since it was a legislation of sectoral application. Roos (n 103above) 23.

105 Kasneci (n 24 above) 16.

106 In 1979, the Federal Data Protection Act came into force.

The evolution of data privacy laws in Germany and Sweden was not coincidental. Certain factors played significant roles in their initial efforts towards data privacy protection. Lloyd points out that these factors were somewhat paradoxical, one defensive and the other permissive.[107] In Germany, the experience of abuse of personal data by the totalitarian regime under the Nazi and at the time of the communist regime in East Germany led to the early recognition of the importance of data privacy. Thus, data privacy legislation was passed for defensive purposes to limit the ability of public and private bodies to process data.

In Sweden, the situation was different. There was no background of a totalitarian regime. However, Sweden had a long standing tradition of freedom of information under which almost any item of information held by public bodies was considered to be in the public domain. Thus, by granting an individual the right of access to data records, data privacy legislation could be seen as extending the concept of freedom of information to the private sector.[108] This shows the permissive role of data privacy. The defensive and permissive roles of data privacy are the two broad functions of the right to data privacy that will be discussed later.

The discussion above shows that Europe has always played a leading role in the development of the right to data privacy globally. The impact of North America is not as significant as that of Europe in this regard, as they tend to always follow the lead of the Europeans in data privacy protection. Yet, most of the data privacy principles as we have them today can also be credited to the efforts of the US Department of Health, Education and Welfare (DHEW) Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens.[109] The report sets out five principles which are a 'Code of Fair Information Practices'.[110] These principles form the

---

107 Lloyd (n 19 above) 22.

108 Lloyd (n 19 above) 22.

109 See US Department of Health Education and Welfare (DHEW) 'Record computers and the rights of citizens' Report of the Secretary's Advisory Committee on Automated Personal Data Systems http://www.justice.gov/opcl/docs/rec-com-rights.pdf (accessed 1 November 2015).

110 US DHEW (n 109 above) xx – xxi. The principles are 1.There must be no personal data record-keeping systems whose very existence is secret. 2. There must be a way for an individual to find out what information about him is in a record and how it is used. 3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. 4. There must be a way for an individual to correct or amend a record of identifiable information about him. 5. Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

normative structure and basis for data privacy practices or fair information principles (FIPs).[111]

Although Africa has had its fair share of totalitarian regimes and military dictatorships, African countries have played an insignificant role towards the emergence and development of the right to data privacy. A number of factors could be the reason for this. One of such reasons is the general African cultural attitude towards privacy. Its communal philosophy has always made Africa take a back seat in the discourse on privacy related issues.[112] With the advances in technology, however, the collectivist culture is quickly disappearing. African countries may therefore play a more significant role in the debate on data privacy in the future. A very low level of awareness of the importance of data privacy protection and associated issues is another reason why African countries have played little or no role in the emergence and development of data privacy. Other factors are technological underdevelopment, poverty and corruption that prevail in many African countries.

2.4.2. Development of the right to data privacy through international instruments

From the 1980s, international institutions began to play an active role in the development of data privacy laws by adopting international instruments. The national instruments at the time had some interrelated shortcomings which were addressed in the international documents.[113] One such shortcoming was the fact that personal data processing was no longer confined to isolated mainframe computers in specific jurisdictions, but was increasingly based on networks[114] connected through the internet. In most cases, these networks included more than one country. A specific national law applicable in one jurisdiction could therefore not deal with all the implications of these transborder flows of personal data. Related to the first limitation of national data privacy laws was the increasing importance of information flow (transborder data flows) across national boundaries. These reasons presented new challenges which national laws could not handle.

---

111 Lessig (n 30 above) 227.

112 More on how culture affects data privacy will be discussed in the next chapter.

113 Lloyd has a different opinion. He states that 'in the data protection context, two- perhaps contradictory- concerns prompted international action. There were fears that national laws, which tended to have strong controls over the export of data, might have protectionist effect. Conversely, there were fears by those states that had adopted data protection legislation that national laws and policies could be circumvented by organisations sending data abroad for processing in countries (often referred to as data havens) which imposed few controls over processing activities.' Lloyd (n 3 above) 27-28.

114 Kasenci (n 24 above) 16-17.

There was thus, the need to ensure a uniform standard across borders for the purposes of free flow of information. This has meant that data privacy law had been always an international issue.[115] In this regard, Roos points out that:

> The internet operates on the principle that information should be able to flow unimpeded over national borders. To allow this, standards for the protection of personal information should be equivalent in all countries connected to the internet. If standards differ, countries with high standards of data protection may decide to impose legal barriers to the transfer of personal information on their citizens to other jurisdictions.[116]

The free flow of information must therefore be facilitated through uniform regulations on data privacy in order to boost international trade. It is obvious that international organisations are well suited for this task. Thus, the Council of Europe (CoE), the Organisation of Economic Cooperation and Development (OECD) and the United Nations (UN) are the main institutions at the international level that have played a significant role in the emergence and development of data privacy law. Each of their contributions will now be discussed in turn.

2.4.1.1.The OECD Privacy Guidelines

At the international level, the OECD[117] was one of the first organisations to have dealt expressly with the data privacy issue.[118] It has, for many decades, played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders.[119] It actually began taking an interest in data privacy at about the same period as the CoE. Work commenced on its draft Regulation, which was undertaken in close liaison with the CoE, in 1969 with the initiation of its computer

115 Roos (n 39 above) 320.
116 Roos (n 39 above) 320-321.
117 The OECD is an international organisation whose main objective 'is to promote policies that will improve the economic and social well-being of people around the world.' It provides a forum in which governments can work together to share experiences and seek solutions to common problems. The OECD works with governments to understand what drives economic, social and environmental change. It measures productivity and global flows of trade and investment and analyses and compares data to predict future trends. It was established in 1961 and it has 34 members which span the globe, from North and South America to Europe and the Asia-Pacific region. See 'about the OECD' http://www.oecd.org/about/ (accessed 1 November 2015).
118 P De Hert & V Papakonstantinou 'Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency?' (2013) 9(2) *I/S: A Journal of Law and Policy for the Information Society* 276.
119 'OECD work on privacy' http://www.oecd.org/sti/ieconomy/privacy.htm (accessed 1 November 2015).

utilisation programme in the public sector.[120] This group carried out studies on electronic data banks, computers and telecommunications. In 1972, a group of experts, the Data Bank Panel, were appointed to analyse different aspects of privacy issues.[121] Another ad-hoc group of experts was set up in 1978 under the chairmanship of Justice MD Kirby, Chairman of the Australian Law Reform Commission.[122] This group developed the Guidelines in the form of a recommendation by the Council of the OECD.[123] The Recommendation was adopted and became applicable on 23 September 1980. Annexed to the Recommendation was the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ('OECD Guidelines').[124]

The OECD notes that new concerns regarding the development of automated data processing with the capability to transfer large amount of data within seconds have led member countries to pass regulations to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.[125] However, that is not the major concern of the OECD. Its major interest in this area is enhancing the free flow of personal data across borders by eliminating impediments caused by disparities in national laws.[126] It is stated in the preface to the recommendation which contains the Guidelines that:

> …there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.[127]

---

120 See Explanatory memorandum to the Guidelines http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation (accessed 1 November 2015). Some versions say work commenced in 1968. See CJ. Bennett & C Raab, *The governance of privacy: policy instruments in global perspective* (2006) 88.

121 Explanatory memorandum to the Guidelines (n 120 above).

122 Explanatory memorandum to the Guidelines (n 120 above).

123 Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980). Available online in http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation (accessed 1 November 2014).

124 (n 123 above).

125 OECD Guidelines (n 123 above).

126 GG Fuster *The emergence of personal data protection as a fundamental right of the EU* (2014)77.

127 OECD Guidelines (n 123 above).

As a consequence of disruption of data flows, member countries should remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data.[128] The above discussion shows that the major motivations for the OECD's work in the area of data privacy are mainly commercial in nature. This is not surprising because the OECD is primarily established to facilitate cooperation between member states in order to promote economic development.

The OECD Guidelines is said to have adopted a common law-based approach to issues as opposed to the CoE Convention which was drafted in the civil law approach.[129] It contains eight broad privacy principles which form the bedrock of data privacy law.[130]

The OECD revised its Guidelines in 2013 to keep pace with the rapid advances in IT. The revision includes a new Recommendation of the OECD Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. This constitutes the first major update to the Guidelines since 1980.[131] There are two predominant themes of the updated Guidelines.[132] The first is that it focuses 'on the practical implementation of privacy protection through an approach grounded in risk management'.[133] Secondly, is recognition of the need 'for greater efforts to address global dimension of privacy through interoperability'.[134] Another important work on data privacy carried out by the OECD is the Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy adopted in 2014.[135] This Recommendation primarily encourages member countries to cooperate across borders in the enforcement of laws protecting privacy.[136]

---

128 OECD Guidelines (n 123 above).

129 Lloyd (n 19 above) 27.

130 The eight principles are the collection principle, data quality principle, purpose specification principle, use limitation principle, security safeguard principle, openness principle, individual participation principle and accountability principle. See generally arts 7-14 of the Guidelines (n 123 above).

131 'Our work on privacy' (n 119 above).

132 OECD 'The OECD privacy framework' (2013) 4. available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed 1 November 2015) 4

133 OECD (n 132 above) 4.

134 OECD (n 132 above) 4.

135 OECD 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy' available at http://www.oecd.org/internet/ieconomy/38770483.pdf (accessed 1 November 2015).

136 Member countries are thus required to take steps to: '(a) Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.(b) Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation. (c) Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing,

The OECD, unlike the CoE, is not established for human rights purposes. It is an international economic institution whose primary objective is to facilitate cooperation between member states in order to promote economic development.[137] As a consequence, commercial and trading interests were its main incentives for its work in the field of data privacy law. This is substantially reflected in the body of the Guidelines as it focuses more on data flow rather than data privacy.

That notwithstanding, the OECD Guidelines is one of the most influential international documents on data privacy today. It serves as a reference point for data privacy frameworks of many countries and institutions. However, it has its own lapses. The first weakness of the Guidelines is that its commercial and economic background has made it inadequate for the purposes of genuine protection of individuals' rights to data privacy. Because of its desire to encourage transborder data flows, emphasis was placed on free movement of data, and individuals' rights have always taken a backseat. Another weakness of the Guidelines is the fact that it is mere guidelines, and as such, not legally binding.[138] In addition, the Guidelines allow considerable variations in implementation by member states. This has brought about different standards in member countries which affects transborder data flow.

2.4.1.2.The Council of Europe's Convention and Additional Protocol

The CoE[139] was also another international organisation to take serious steps towards data privacy protection.[140] In 1968, the Committee of Ministers of the CoE were faced with a request (Recommendation 509) from the Parliamentary Assembly to consider the extent to which the provisions of the European Convention on Human Rights (ECHR)[141] and

---

subject to appropriate safeguards. (d). Engage relevant stakeholders in discussion and activities aimed at furthering cooperation in the enforcement of laws protecting privacy.' OECD (n 135 above) 7.

137 See 'about OECD' (n 117 above). See also Lloyd (n 3 above) 31.

138 Roos (n 39 above) 324. Fuster (n 126 above) 80-81.

139 The Council of Europe (CoE) is Europe's leading human rights organisation with headquarters in Strasbourg, France. It has 47 members, 28 of which are members of the EU. The CoE's entire member states have signed and ratified the European Convention on Human Rights (ECHR) which is a treaty designed to protect human rights, democracy and rule of law. CoE 'The Council in brief' http://www.coe.int/en/web/about-us/who-we-are (accessed 1 November 2015).

140 LA Bygrave *Data privacy law: An international perspective* (2014)31.

141 Convention for the Protection of Human Rights and Fundamental Freedoms (1950) available at http://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed 1 November 2015).

domestic laws protected individuals against abuse of modern science and technology.[142] The assembly observed the obvious weaknesses of the ECHR together with the Universal Declaration of Human Rights (UDHR)[143] in addressing violations of human rights brought about by the emergence of new technologies.[144] Based on the report of the Assembly, two separate resolutions were adopted by the Committee of Ministers regarding private[145] and public sectors.[146] Both resolutions recommended that national laws should contain the FIPs, particularly, the requirements for lawful processing and for individual access. These principles underpin data privacy laws till date. With time, advances in IT exposed the shortcomings of the resolutions.[147] The resolutions did not prescribe the means by which member states should give effect to the principles. Consequently, there were large scale discrepancies in member states' data privacy laws.[148] This led to a move towards a treaty to ensure better harmonisation of national laws.

The ensuing treaty, the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data ('CoE Convention')[149] was adopted in Strasbourg and opened for signature in January 1981. It was to come into force on ratification by five member states which happened only in October 1985.[150] The Convention has, over time, undergone several amendments to keep pace with emerging challenges. There is also an Additional Protocol regarding Supervisory Agencies and Transborder Data Flows ('the Additional Protocol').[151] As of October 2014, forty six (46) countries have ratified the CoE

---

142 Para 4 of the Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1980) available at http://conventions.coe.int/Treaty/en/Reports/Html/108.htm (accessed on 1 November 2015).

143 Adopted in 1948 by the United Nations General Assembly, Resolution 217 A (III).

144 And domestic laws, See (n 118 above) para 4

145 Resolution (73) 22 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in Private Sector (adopted 26 September 1973).

146 Resolution (74) 29 on the Protection of Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Private Sector(Adopted 24 September 1974).

147 '[T]he resolution and most subsequent data protection law, are based on the notion of a single controller with a single computer holding data. This bears little resemblance to today's networked environment. In particular, reactive controls may not be sufficient. Once inaccurate data has found its way onto the internet, the damage can never be undone.' See Lloyd (n 19 above) 25.

148 Lloyd (n 19 above) 25.

149 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108 at http://conventions.coe.int/Treaty/en/Treaties/html/108.htm (accessed 1 November 2015). It is also sometimes referred to as Convention 108. See Bygrave (n 140 above) 31-32.

150 Lloyd (n 19 above) 25.

151 Titled 'Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows.' It was opened for signature in Strasbourg on 8th November 2001. It came into force after receiving five members state ratified on the 1/7/2004. See http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=8&DF=23/10/2014&CL=ENG (accessed 1 November 2015).

Convention and thirty five (35) have ratified the Additional Protocol.[152] Even though the Convention has a European origin, it allows countries who are non-members of CoE to be signatories. Based on article 23 of the Convention, the CoE's committee of ministers may invite non-members to accede to the Convention.[153]

The Convention covers all processing of personal data of physical persons in both the private and public sectors. It does not apply to juristic persons. Member states may, nevertheless, extend the application of the Convention to the processing of data 'relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.'[154] The Convention's scope is also restricted to automated or computerised processing of personal data. It does not cover manual processing. Member States may nevertheless extend the application of the Convention to non-automated or manual processing of personal data.[155]

Some shortcomings have been identified with the Convention such as the lack of regulation of the flow of personal data from a party to non-party state and the lack of provisions requiring the establishment of Data Protection Authorities (DPAs) in the party states. Also, the Convention does not provide for an overall oversight and enforcement authority similar to the Article 29 Working Party.[156] In addition, the basic principles of data protection (the FIPs) are formulated in a general, abstract way, and many key terms are left undefined by the Convention and its explanatory report.[157] Most of these criticisms were, however, taken care of by the Additional Protocol.[158] At present, there are still more developments with regard to the Convention.

There are currently proposals on the table for the 'modernization' of the Convention. These proposals were forwarded from the Convention's Consultative Committee (T-PD) to

---

152 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures (accessed 1 November 2015).

153 In 2011, Uruguay became the 1st non-state member followed by Morocco in 2013.

154 Art 3(2)(b) of the CoE Convention.

155 Art 3(2)(b) of the CoE Convention.

156 Bygrave (n 140 above) 40.

157 Bygrave (n 140 above) 40.

158 Eg, art 2 of the Additional Protocol provides for 'Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a party to the Convention' similarly, art 1 provides for 'supervisory authorities'.

the Council of Ministers for consideration.[159] Most of the proposed changes are aimed at strengthening the Convention.[160] These changes also aim to incorporate the provisions of the Additional Protocol into the Convention itself.[161] Other changes proposed to the Convention include: strengthening the obligation of the parties to implement the Convention; tightening existing data protection principles and adding new principles to bring the Convention in line with the EU Directive and the newly proposed draft EU Regulation; and strengthening the powers of the supervisory authorities.[162] A new committee called the Convention Committee is given the mandate of assessing proposed parties (state parties) for accession and reviewing the level of implementation of the Convention by existing parties. This shows that the Convention is being given a 'facelift' in order to make it effective in protecting individuals from threats with regard to the processing of their personal information.

The CoE remains one of the few international institutions which have drafted a multilateral treaty directly on the right to data privacy.[163] The Convention is the only binding global data privacy legal document. Efforts are being made to make it more of a global privacy agreement open to all countries that provide the required level of data protection.[164] Commentators, like Greenleaf, are optimistic that with the proposed amendments in the Convention, the vacuum created by the absence of a global data privacy treaty will be filled.[165] The proposed amendments will furthermore allow countries outside Europe to play a more significant role in the development of data privacy law. Nevertheless, as noted

---

159 CoE 'Consultation committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (T-PD) Final Document on the modernisation of Convention 108 available at https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04_rev2_En.pdf (accessed 1 November 2015). For more elaborate discussion on the 'modernisation' and 'globalisation' of the Convention, see G Greenleaf "'Modernising' Data Protection Convention 108: A safe basis for a global privacy treaty?" (2013) 29 *Computer Law & Security Review* 430-436.

160 It is still unclear when the proposals will fully take effect. The website of the CoE, however, states that they are supposed to enter into force on the 1st of September 2015. http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp (accessed 1 November 2015).

161 Greenleaf (n 159 above) 431, so that it will not be possible to ratify one without the other as was done by some countries like Morocco.

162 Greenleaf (n 159 above) 431

163 Greenleaf (n 159 above) 431. The African Union has also adopted a Convention which will be considered shortly.

164 G Greenleaf 'Morocco and Uruguay start Convention 108's journey to global privacy Treaty' (2013) 122 *Privacy Laws & Business International Report* 20-23.

165 Greenleaf (n 159 above).

by Greenleaf, 'the success of globalization depends largely on the perceptions of non-European states, and whether they wish to apply to accede to the Convention'.[166]

The status of the CoE's Convention as a human rights document has been controversial. Some US commentators have expressed the view that the provisions of the Convention were motivated by commercial expediency and economic factors, rather that genuine concern for individuals' right to data privacy.[167] Put in another way, it has been argued that the data privacy right of individuals was a secondary objective of the Convention. Lloyd rejects the argument and points out that 'the Convention, as with much of the Council of Europe's work, is deeply rooted in the human rights context and specifically in the European Convention of Human Rights'.[168] Fuster also holds a similar view where she contends that the Convention has formally one single purpose - safeguarding the human right to data privacy.[169]

2.4.1.3.The UN Privacy Framework

The UN has also played some role in the development of the *sui generis* right to data privacy, though not as substantial as the previous two international institutions. The initial initiative of the UN in the field of data privacy law was based on a resolution of the General Assembly inviting the Secretary General to consider individuals' right to privacy in the light of advances in recording and other techniques.[170] This led to a publication of a report encouraging states to adopt data privacy legislation.[171] In the early 1990s, the United Nation's Economic and Social Council agreed to the Guidelines Concerning Computerized Personal Data files ('the UN Guidelines').[172] In line with the OECD Guidelines and the CoE Convention, the UN Guidelines contain ten principles for lawful processing of personal data which are the 'minimum guarantee that should be provided in national legislation.'[173] Lloyd notes two striking features of the UN Guidelines.[174] Firstly,

166 Greenleaf (n 159 above) 12.
167 Lloyd (n 3 above) 29.
168 Lloyd (n 3 above) 30. See also C de Terwangne 'Is a global data protection regulatory model possible?' in S. Gutwirth *et al* (eds) *Reinventing data protection?* (2009) 180.
169 Fuster (n 126 above) 89. Although, she subsequently argues that the Convention also encourages TBDF.
170 Bygrave (n 140 above) 51.
171 Bygrave (n 140 above) 51.
172 Guidelines for the regulation of computerized personal data files A/RES/45/95 adopted by the UN General Assembly (GA) on 14 December 1990. Available at http://www.refworld.org/docid/3ddcafaac.html (accessed 1 November 2015).
173 They are the principle of lawfulness and fairness, principle of accuracy, principle of the purpose-specification, principle of interested-person access, principle of non-discrimination, power to make

provisions are made for the application of the principles by international agencies[175] and secondly, the principles apply to manual processing of data as well as to legal persons.[176]

The UN has recently made more of an effort to play an active role in the field of data privacy.[177] There have been two recent UN General Assembly Resolutions on *Privacy in the digital age* in 2013[178] and 2014.[179] It is based on the recent UN initiatives that Zalnieriute argues that data privacy has indeed crystallised into a norm of customary international law.[180] There are also calls for the adoption of a global data privacy framework under the auspices of the UN by some commentators like De Hert and Gutwirth[181] and Kuner.[182] This may, however, not be easy to realise especially because of the fundamental divergence in values attached to privacy by the major players in the field.[183]

As stated above, the influence of the UN Guidelines on the field of data privacy law was less significant than that of the CoE Convention and the OECD Guidelines. Bygrave notes that its 'soft law' status may be a part of the reason for this, but only to a small degree since the more influential OECD Guidelines is also a soft law.[184] He argues that the UN Guidelines' greater strictness on important aspects compared to the other two documents is a significant factor. So too is the fact that the absence of definitions of key terms in the Regulation means that it is less useful in practical situations.[185]

---

exceptions, principle of security, supervision and sanctions, transborder data flows and field of application. See part A of the UN Guidelines

174 Lloyd (n 3 above) 33.

175 See part A, para 10 of the UN Guidelines.

176 Para 10 of the UN Guidelines.

177 Eg, at a meeting of data protection and privacy protection commissioners, a proposal was endorsed encouraging the adoption of 'international standard for the protection of privacy and personal data'. Also in 2010, the UN Rapporteur on human rights made a call for the establishment of global privacy standards. See Lloyd (n 3 above) 33.

178 See General Assembly Resolution A/RES/68/167 on the Right to Privacy in the Digital Age adopted on 18 December 2013 available at http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed 1 November 2015).

179 General Assembly Resolution A/RES/69/166 on the Right to Privacy in the Digital Age adopted on 18 December 2014 available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166 (accessed 1 November 2015).

180 M Zalnieriute 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) 0 *International Journal of Law and Information Technology* 1-35.

181 De Hert & Papakonstatinou (n 118 above)

182 Kuner (n 37 above) 315.

183 See Kuner (n 37 above) 315, 316; L Bygrave 'International agreement to protect personal data' in JB Rule & G Greenleaf *Global privacy protection* (2008) 48-49.

184 Bygrave (n 140 above) 53.

185 Bygrave (n 140 above) 53.

2.4.3. Development of the right to data privacy through regional instruments

The challenge of getting a harmonised data privacy instrument at international level resulted in data privacy increasingly becoming a regional issue. Numerous regional organisations play active roles in the development of the right to data privacy. For the purpose of this section, instruments emanating from three main regional groupings will be considered. They are the European Union (EU),[186] the Asia-Pacific Economic Cooperation (APEC) and African Union (and other African sub-regional organisations).

2.4.3.1. The EU Directive, EU Charter and the draft EU Regulation

Of all the regional organisations, the EU[187] has made the most significant contribution to the development of the right to data privacy. Its most important contribution was in the early 1990s with the adoption of the EU Directive in 1995 which came into force in 1998. The Directive is considered to be the most comprehensive and successful international instrument on data privacy.[188] It is currently the leading force in the globalisation of data privacy law.[189]

The adoption of the EU Directive resulted from a series of proposals urging the then European Community (EC) to take action regarding data privacy protection because of perceived threats from emerging technologies.[190] The European Parliament played an active role in this regard. It made several calls for the drafting of a directive and for members to sign and ratify it.[191] The European Commission, along with the Council of

---

186 Many scholars will classify EU as an international institution because of its significant contribution to the development of data privacy law. I choose to classify it as a regional institution for the purpose of clarity. This is due to the fact that despite its significant influence, its scope of application is only restricted to member states in Europe. Arguably, so also the CoE, however, the CoE allows non-European countries to be parties to it. It therefore prevented its classification as a regional organisation.

187 The European Economic Community (EEC) was created by the Rome Treaty of 1957 so as to bring about economic integration in Europe by establishing a common market among its member states. In 1993, it was renamed the European Community (EC) by the Maastricht Treaty. In 2009, the EC was succeeded by the European Union (EU) through the Treaty of Lisbon. The EU is a unique economic and political partnership between 28 European countries that cover most of the continent. It initially began as a pure economic union, but it has overtime expanded its scope to cover policy areas such development and environment. Its single or 'internal' market is the EU's economic engine. This enables goods, services, money and people to move freely through most of the continent. Recently, it has extended its functions to human rights. See generally 'How the EU works' http://europa.eu/about-eu/ (accessed on 1 November 2015).

188 Bennett & Raab (n 120 above). Bygrave (n 140 above) 55.

189 Birnhack (n 25 above)512.

190 Bygrave (n 140 above) 54.

191 Bygrave (n 140 above) 54.

Ministers, was more reluctant as it was more focused on the development of the internal market and a European computer industry.[192]

In 1981, the EC issued a recommendation calling on the Parliament to sign and ratify the CoE Convention.[193] By the end of 1981, the Commission started work on a framework directive on data privacy. The Commission took the work more seriously when it realised that the uneven nature of regulations on data privacy in member states could affect the aim of realisation of the internal market which is a fundamental objective of the EC. In 1990, the EC issued its first proposal for a Framework Directive on data privacy.[194] This proposal was severely criticised, hence the Commission issued an amended proposal in 1992. Three years later, the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard To the Processing of Personal Data and on the Free Movement of Such Data ('the EU Directive') was adopted. [195] Though, the Directive has been approved by the EU, it is not self-implementing.[196] Each member state must enact its own implementing legislation before it takes effect in the individual jurisdictions.[197]

In 2000, the Charter of Fundamental Rights of the European Union ('the EU Charter')[198] was enacted and, for the first time, data privacy was recognised as a fundamental human right independent of the right to privacy.[199] It has been argued that the inclusion of the fundamental right to data privacy was to substantiate the human rights objective of the

---

192 See Bygrave (n 140 above) 54-55.

193 Commission Recommendation 81/679EEC relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data [1981] OJ L246/31 available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31981H0679&from=EN (accessed 1 November 2015).

194 Proposal for a Council Directive Concerning the Protection of Individuals in relation to the Processing of Personal Data [1990] OCJ C277/3

195 Available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:31995L0046 (accessed 1 November 2015). For insightful discussions on the EU Directive, see Y Poullet 'The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206-217; N Robinson *et al* 'Review of European Data Protection Directive' (2009) Technical report of Rand Europe, available at http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf (accessed 1 November 2015); R Wong 'The Data Protection Directive 95/46/ EC: Idealisms and realisms' (2012) 26 *International Review of Law, Computers & Technology* 229-254.

196 JM Fromholz 'The European Union Data Privacy Directive' (2000) 15 *Berkeley Technology Law Journal* 467-468.

197 Fromholz (n 196 above) 467-468.

198 Charter of Fundamental Rights of the European Union (2000/C 364/01) available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 1 November 2015).

199 Art 8 of the Charter. See also art 16 of Treaty for the Functioning on the European Union (TFEU). See also GG Fuster & R Geller 'The fundamental right of data protection in the European Union: In search of an uncharted right' (2012) 26 *International Review of Law, Computers & Technology* 73-82.

Directive.[200] This is because the Directive has a 'dual personality': it is aimed at both market integration and human rights. Nevertheless, the separation of the right to data privacy from the right to privacy should be welcomed because of the 'added value' of the right to data privacy.[201] This Charter did not, however, take effect until 2009 when the Lisbon Treaty came into force.[202]

To further strengthen the EU data privacy regime, especially its human rights agenda, the Directive is currently under review. The reform, which is still on-going, is contained in the a '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 ('draft EU Regulation' or 'draft Regulation')'. [203] Another reason for the review, according to the EU Data Protection Supervisor (EDPS), is the need to update the current framework so as to ensure continuous effectiveness in practice and the need to increase harmonisation.[204] Unlike the Directive, the draft Regulation will have a direct effect on member states without the need to be transposed into national law.[205] The draft Regulation has, however, been criticised as based on certain fallacies which makes it unrealistic.[206]

One of the main issues regarding the EU regime is its extraterritorial effect. Concerns have been raised that the EU is attempting to legislate for the whole world with its data privacy

---

200 P De Hert & S Gutwirth 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in S Gutwirth *et al* (eds) *Reinventing Data Protection?* (2009) 8.

201 P De Hert & S Gutwirth 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes *et al.* (eds), *Privacy and the criminal law* (2006) 61.

202 Adopted on 13th December 2007 and came into force on 1st December 2009. The Treaty of Lisbon came into force to reform the two basic EU treaties which are Treaty on the European Union and Treaty Establishing the European Community.

203 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/2012/011 final - 2012/0011 (COD) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011 (accessed 1 November 2015) For more on the draft EU Regulation, see P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Report* 130-142; Van der Sloot (n 22 above) 307-325.

204 PJ Hustinx '(Future) interaction between Data Protection Authorities and National Human Rights Institutions in the European Union' in J Wouters & K Meuwissen (eds.) *National human rights institutions in Europe. Comparative, European and international perspective* (2013) 165.

205 Van der Sloot (n 22 above) 318. For more on the legal effect of regulations generally in the EU legal order, See E Rotondo 'The legal effect of EU Regulations' (2013) 29 *Computer & Security Report* 437-445.

206 B Koops 'The trouble with European data protection law' (2014) 4(4) *International Data Privacy Law* 250-261. See also Bergkamp (n 34 above).

regime.[207] This is because of the provisions of articles 25 and 26 of the EU Directive. These provisions attempt to closely track the flow of European's personal data by ensuring that only non-EU countries with an 'adequate' level of protection of personal data may receive Europeans' personal data for processing.[208] These provisions sparked controversies between European and non-European scholars. Non- European scholars contend that the EU is trying to impose its standards on the world.

To say that Europe, through the EU Directive, is trying to legislate for the whole world may be an attractive argument. This is because of the significant influence it has on data privacy regimes in many jurisdictions across the globe.[209] However, such argument may not be the best way to describe the influence of the Directive. Legislating for the whole world implies it is forcefully imposing its regime on other jurisdictions. However, the EU Directive, though highly influential, does not force its regime on other countries. Article 25 expressly prohibits the transfer of data to non-EU countries without adequate protection of personal data. However, article 26 provides an alternative process, albeit cumbersome, for such transfers to be effected. Thus, countries without 'adequate' data privacy legislation are free to resort to the provisions of article 26 so as to receive data from the EU. The EU can at best be said to apply 'a sophisticated, inducing mechanism to spread its gospel.'[210]

2.4.1.4.The APEC Privacy Framework

The APEC[211] member economies[212] started to move the APEC processes in the direction of a regional privacy agreement in late 2002.[213] Its primary instrument, the APEC Privacy

---

207 Bygrave (n 183 above) 15; AB Makulilo '"One size fits all": Does Europe impose its data protection regime on Africa?' (2013) 7 *Datenschutz und Datensicherheit* 447

208 Birnhack (n 25 above) 512.

209 Birnhack (n 25 above) 515. He contends that '[a] decade after the Directive entered into force, it is time to acknowledge that it has had a wider global impact than thus far acknowledged'.

210 Birnhack (n 25 above) 512.

211 APEC was established in 1989 to enhance growth and prosperity for the region and to strengthen the Asia-Pacific community. It is the leading forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific Region. APEC is an intergovernmental grouping that operates on the basis on non-binding commitments, open dialogue and equal respect for the views of members. It has no treaty obligation requirement for its member economies. Decisions made within APEC are reached by consensus and commitments are undertaken on voluntary basis. It has 21 members which account for about 40% of the world's population. See 'About APEC' http://www.apec.org/About-Us/About-APEC.aspx (accessed 1 November 2015).

212 According to the APEC website, '[t]he word 'economies' is used to describe APEC members because the APEC cooperative process is predominantly concerned with trade and economic issues, with members engaging with one another as economic entities.' http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (accessed 1 November 2015).

Framework, was adopted in 2004.[214] It is the most significant international data privacy instrument adopted since the EU Directive.[215] The framework is, to a large extent, based on the OECD Guidelines rather than the CoE Convention or the EU Directive.[216] It is not surprising that the Framework is described as 'OECD lite'.[217] The APEC's Framework, according to Bygrave, focuses more on engendering consumer confidence in business than on the human right to data privacy.[218] Thus, economic considerations are dominant in the Framework.

The APEC Privacy Framework has nine 'information privacy principles' which have shown significant influence from the OECD Guidelines, but it also contains new principles, arguably not found in any other data privacy instrument.[219] The standard set by APEC is generally lower than the EU standard. Greenleaf points out that APEC's implementation proposals are so non-prescriptive that they amount to no standards at all.[220] A reason for this may be because APEC operates on a non-binding basis. This is demonstrated by its choice of a 'framework' rather than a 'guideline' or 'convention'. Hence, APEC's framework has a considerably less influence on the development of data privacy law than other data privacy instruments have. Moreover, it has an even lesser influence on the data privacy regimes in member economies who prefer to rather adopt the EU model.[221] Greenleaf opines that the US played a role in the relative weak standards of the APEC so as to impede the spread of strong data privacy laws.[222]

---

213 G Greenleaf 'APEC's privacy framework sets a new low standard for Asia-Pacific' in AT Kenyon & M Richardson (eds) *New dimensions in privacy law: International and comparative perspectives* (2006) 94.

214 The instrument was the tenth version. It was adopted by APEC Ministers in November 2004. The privacy framework is available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (accessed 1 November 2015).

215 Greenleaf (n 213 above) 91.

216 The Preamble of the Privacy Framework shows the APEC's affiliations with the OECD. It provides that the Framework aims at promoting electronic commerce throughout the Asia Pacific region and is consistent with the core values of the OECD Guidelines. See APEC Privacy Framework (n 214 above) para 5.

217 Greenleaf (n 213 above) 96. It is termed 'OECD lite' because it contains provisions similar to the OECD Guidelines, but the provisions have been significantly watered down.

218 Bygrave (n 140 above) 75.

219 Eg, the principles of 'Preventing Harm' (Principle I); 'Choice' (Principle V); and 'Accountability' concerning data exports (Principle IX). See G Greenleaf 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108' (2012) 2(2) *International Data Privacy Law* 63. For more in depth analysis of the principles, See Bygrave (n 140 above) 76.

220 Greenleaf (n 213 above) 93.

221 G Greenleaf 'Asia-Pacific data privacy: 2011, year of revolution?'(2011) *Kyung Hee Law Journal*. see also Greenleaf (n 219 above).

222 Greenleaf (n 219 above).

2.4.1.5.The African instruments

African regional bodies have been very silent in the field of data privacy law. The African Union (AU), which is the primary regional body in Africa, has not made any serious impact in the field of data privacy law, until very recently. The AU adopted the African Union Convention on Cyber-security and Personal Data Protection.[223] A perusal of the Convention shows that it has a very wide scope. Data privacy, in this researcher's view, is only treated as incidental to achieving cyber security. Nevertheless, it may be too early to evaluate the actual impact of the Convention.[224]

At the sub-regional level, the Economic Community of West African States (ECOWAS), through its Supplementary Act 2010 on Data Protection[225] plays a leading role. However, it has no significant influence in the region in spite of the fact that the Supplementary Act is an integral part of the ECOWAS Treaty[226] and legally binding on member states.[227] In the Southern African sub-region, there is the Southern African Development Community (SADC) Data Protection Model Law 2012.[228] Makulilo points out that although 'these instruments are likely to influence the development of data protection law in Africa, doubts have been cast on their ability to do so.'[229] Be that as it may, it must be admitted that Africa is gradually growing in the field of data privacy law especially with the recent adoption of the AU Convention.[230]

2.4.4. The influence of other international human rights instruments on the development of the right to data privacy

Certain international and regional human rights instruments have influenced the emergence and development of the right to data privacy, notable among which are the Universal Declaration of Human Rights (article 12), the International Covenant on Civil and Political Rights 1966 (article 17) and the European Convention on Human Rights 1950

---

223 This was at the AU submit in Malabo, Equatorial Guinea. The Convention is available at http://pages.au.int/sites/default/files/AU%20Cybersecurity%20Convention%20ENGLISH_0.pdf (accessed on 1 November 2015).

224 More elaborate discussion on the Convention will be carried out in the next chapter.

225 A/SA.1/01/10. Also available at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf. (accessed 1 November 2015).

226 Art 48 of the ECOWAS Supplementary Act.

227 The Act will be considered in more depth in the next chapter.

228 Makulilo (n 207 above) 450.

229 Makulilo (n 207 above) 450

230 See generally G Greenleaf & M Georges 'The African Union's Data Privacy Convention: A major step toward global consistency' (2014) 131 *Privacy Laws & Business International Report* 18-21.

(article 8). These instruments, which provide for the broad notion of a right to private and family life, form the normative basis of the right to data privacy. They are also increasingly used as data privacy instruments in themselves.[231] However, they are general human rights documents. This section (and the thesis) focuses on instruments that specifically deal with the *sui generis* right to data privacy. That notwithstanding, the contributions of these documents in the development of data privacy right cannot be underestimated.

2.5. Data privacy as a human right or commercial issue?

Data privacy law is increasingly becoming a very important issue. However, it is generating numerous debates in its emergence and development as a field of law. One very relevant debate is about its status as a human right. There is still a controversy regarding the relationship between data privacy and human rights.[232] This controversy arises because of the broad and vague objectives of data privacy legal instruments.

Without a doubt, one of the initial drives for the regulation of personal data processing was commercial or business related. With the increasing profile of personal data as a commodity, it continued to attract more attention in commerce. It was increasingly needed both within and outside the borders of states. Countries therefore enacted data privacy laws to enhance the flow of personal data. Indeed, Bygrave notes that the fear of disrupted data flows probably had the most significant impact in stimulating the adoption of international data protection instruments, especially the OECD Guidelines and the EU Directive.[233] There was also the issue of economic protectionism. According to Caruana and Cannataci, countries, especially those under treaty obligations to reduce tariff barriers, were apprehensive that others might use national data privacy laws as a non-tariff barrier.[234] Thus, data privacy laws were seen to serve economic protectionist purposes. Another fear, which is of a purely economic character according to Bygrave, is the possibility that 'in the

---

231 Bygrave (n 83 above) 45. See also LA Bygrave 'Data protection pursuant to the right to Privacy' 6(3) *International Journal of Law and Information Technology* (1998).

232 Human rights in the digital age are generally provoking so much controversy today. R Mansell 'Human rights and equity in cyberspace' in A Murray & M Klang *Human rights in the digital age* (2005) 1.

233 Bygrave (n 140 above) 10-11.

234 MM Caruana & JA Cannataci 'European Union privacy and data protection principles: Compatibility with culture and legal frameworks in Islamic states' (2007) 16 *Information & Communications Technology Law* 105.

absence of data privacy law, the general populace will lack the confidence to participate in commerce, particularly as consumers / prosumers'.[235]

All the above make commentators doubt the status of data privacy as a human rights issue. Besides, there is a gulf of divide between countries which view data privacy issues from the economic perspective and those that see data privacy as deeply rooted in the notions of human rights.[236] The pertinent question therefore is: is data privacy a commercial issue or a human rights issue which transcends economics and commerce?

In a seeming reply to the above query, Craig and Ludloff argue that the question depends on what (data) privacy means to each of us which is determined by our unique life experiences, culture, society, politics, religion, race and gender.[237] They contend that various countries align along either one of the two paths (commercial and human rights).[238] The commentators further opine that the US treats data privacy as a commodity that can be sold and bought, while the Europeans and many other countries see data privacy as a basic human right equivalent to other freedoms. [239]

The question of whether data privacy is treated as an economic issue or a human rights issue is crucial, as it affects the approach to the regulation of data processing. A determination that data privacy protection is for the purposes of economic successes will naturally have the effect of relegating privacy and autonomy to the background.[240] Consequently, if a legal instrument on data privacy has pure economic motives, so much attention will be placed on enhancing data flows at the expense of human right. On the other hand, if a data privacy law is 'rights-based', greater emphasis will be on the protection of individuals' rights to data privacy. [241]

The EU Directive, which is the most influential and successful data privacy instrument, also plays a role in this controversy. This is because the Directive has been argued as being more for commercial purposes than human rights. The reason for this contention is that the

---

235 Bygrave (n 140 above) 11.
236 Lloyd (n 3 above) 33.
237 Craig & Ludloff (n 11 above) 68.
238 Craig & Ludloff (n 11 above) 68.
239 Craig & Ludloff (n 11 above) 68.
240 Bernal states that '[s]o long as the primary focus remains on economic success, privacy and autonomy are likely to be squeezed…' PA Bernal 'Do deficiencies in data privacy threaten our autonomy and if so, can informational privacy rights meet this threat?' published PhD thesis, London School of Economics and Political Science, 2011 268.
241 Bernal (n 32 above) 223.

EU was originally established as a market integration institution. Hence, its competence to legislate in the field of human rights is uncertain.[242] Moreover, the Directive places so much emphasis on its market objective rather than human rights.[243] The Directive refers to economic and social progress and trade expansion[244] and the free flow of personal data[245] alongside the right to privacy.[246] This may therefore create the impression that the commercial agenda of the Directive is preeminent. Hence, the EU Directive may be argued not to be 'rights-based'. Bernal is one of the scholars who hold this view. His contention regarding the EU regime generally is that:

> In principle it is 'rights-based', at least in the sense that its origins include Article 8 of the European Convention on Human Rights, the rights to respect for privacy (embracing a right to a private life). In practice, however, data protection is more about the regulation of data flow than the protection of individuals' privacy, and it is treated to a greater extent as a piece of technical legislation to be complied with rather than as a statement of rights and principles, and though the proposed new data protection regulation has more of a focus on individual rights, it remains focused on the data than the individual.[247]

Notwithstanding the forgoing, there are numerous arguments in favour of the fact that data privacy, and the EU regime is, at least recently, rights-based.[248] Kuner, for example, contends that the normative basis of data privacy relies heavily on human rights documents.[249] Based on this, it is arguable that data privacy is a human right since it evolved from human rights instruments. Without doubt, data privacy regulation seeks to regulate transborder data flow and enhance the free flow of information in the digital society. Its status as a human right, however, cannot be denied. This is because data privacy is one of the main subject areas of international institutions which have human rights protection as a core function. The UN and the CoE have drafted instruments on data privacy based on their promotion of human rights mandates.

---

242 Indeed Fuster notes that '[t]he original Treaties establishing the European Communities did not contain any explicit reference to human or fundamental rights' (n 126 above) 164.

243 See eg, recital 3 of the Directive which provides that '[w]hereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.'

244 Recital 2, 56.

245 Art 1(2).

246 Recital 2, 9-11, 68 and art 1(1).

247 Bernal (n 32 above) 223.

248 See Lynskey (n 6 above) 73, Rodotà (n 1 above) 77-82.

249 Kuner (n 37 above) 309.

The argument that data privacy is a human right is further strengthened by the fact that there are calls for an international legal framework for the human right to privacy and data protection under the umbrella of the UN. This was part of the 'Montreux Declaration' in which an appeal was made 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'.[250] Many Data Protection Authorities (DPAs) also view data privacy as a human right of universal application.[251] In the Strasbourg Resolution for example, it was unequivocally stated that 'the rights to data protection and privacy are fundamental rights of every individual irrespective of his nationality or residence'.[252]

Any doubt regarding the status of data privacy as a human right seems to have been settled with the endorsing of a fundamental right to data privacy in the EU legal order. The EU Charter provides for an independent right to data privacy separate from the right to privacy.[253] The Treaty of the Functioning of the EU (TFEU) also provides for a directly applicable right to data privacy.[254] De Hert and Gutwirth contend that the incorporation of data privacy as a fundamental right in the Charter of the EU is to substantiate the human rights basis of data privacy in the EU which was hitherto heavily contested.[255] The jurisprudence of the Court of Justice of the European Union (CJEU) has also shown a gradual move from a market to a strict human rights objective especially after the coming into force of the Lisbon Treaty.[256] Moreover, the right to data privacy is increasingly being incorporated as a fundamental human right in the constitutions of countries.[257] This shows a gradual move to a truly rights-based approach to data privacy protection.

---

250 De Terwangne (n 168 above) 175-176. See also Kuner (n 37 above) 308.

251 De Terwangne (n 168 above) 175-176.

252 See (n 7 above).

253 This act of the EU has been criticised. Bergkamp argues that: 'An unfortunate consequence of including this right among truly fundamental rights, such as the prohibition of torture and slavery and the freedom of expression, is that the notion of fundamental right seriously devaluates, with adverse consequence for the respect for core human rights.' Moreover the Charters provision on the right to data privacy is too explicit and detailed for a bill of right. (n 34 above)33.

254 See art 16 of the TFEU.

255 De Hert & Gutwirth (n 200 above) 8.

256 Lynskey (n 6 above) 73.

257 Egs are Portuguese Constitution, art 26; the Federal Constitution of the Swiss Confederation, art 13; The Constitution of the Kingdom of Netherlands, art 10. More recently, the Kenyan Constitution has incorporated the right to data privacy, however, subsumed under privacy. See the Constitution of Kenya 2010, sec 31(c).

2.6. Distinguishing the right to data privacy from the 'traditional' right to privacy: A conceptual debate

The right to data privacy is a unique right which seeks to protect individuals from harm resulting from the processing of their personal data. Its main objective, according to most data privacy instruments, is to secure the privacy related interests in data that can reasonably identify an individual. This objective of data privacy raises the question of the exact nature of the relationship between this relatively new right and the traditional right of privacy, that is, the right to private and family life. Questions in this regard are: is the right to data privacy subsumed under the right to privacy or is it an independent right, totally different from the right to privacy? These questions are fundamental for a proper appreciation of the rudiments of data privacy and the interest(s) it seeks to protect.

The controversies regarding the nature of the relationship between both rights seem to have arisen in Europe. This is because of the EU Charter's introduction of the right to data privacy independent of the right to private and family life.[258] The separation of these two rights distinguishes the EU Charter from other international human rights instruments, since in these instruments, the right to data privacy protection is usually not explicitly provided for. In the case of the EU Charter, 'the constitutional lawmaker goes one step further to provide for an independent fundamental right [to data privacy].'[259] Fuster contends that after the proclamation of the EU Charter, literature started to increasingly acknowledging data privacy as an independent human right.[260] Thus, this action of EU Charter has generated numerous academic debates.[261] It may be asked what the rationale for the separation of these two rights in the EU Charter is. This question may help provide a guide to the type of the relationship or differences between these two rights. The EU

---

258 Art 8 of the EU Charter provides for the right to data privacy (data protection) while art 7 provides for the right to privacy. Similarly, art 16 of the Treaty on the Functioning of the European Union (TFEU) as introduced by the Lisbon Treaty also provides that everyone has the right to the protection of personal data concerning him or her. http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf (accessed 1 November 2015)

259 De Hert & Gutwirth (n 200 above) 6.

260 Fuster (n 126 above) 214

261 See O Lynskey 'Deconstructing data protection: the 'Added-value' of a right to data protection in the EU Legal order' (2014) *International and Comparative Law Quarterly* 569-597.; AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2 *International Data Privacy Law* 164-167; M Tzanou 'Data Protection as a fundamental right next to privacy? "Reconstructing" a not so new right' (2013) 3 *International Data Privacy Law* 88-99; J Kokott & C Sobotta 'The distinction between privacy and data privacy in the jurisprudence of the CJEU and EctHR' (2013) 3(4) *International Data Privacy Law* 222-228; LA Bygrave 'The place of privacy in data protection law' (2001) 24 *UNSW Law Journal* 277-283.

Directive is not helpful in this regard, as it makes no reference to the right to data privacy.[262] The lack of reference to data privacy in the Directive is not surprising because it was enacted long before the EU Charter which was proclaimed only in 2000. Anticipatory reference by the EU Directive to the EU Charter is therefore unlikely. The Explanatory Memorandum[263] to the EU Charter is also unhelpful in seeking the justification for the separate provisions for both rights.[264] It merely states that article 8, which provides for the right to data privacy, is based on article 286 of the Treaty Establishing the European Community, the EU Directive, article 8 ECHR and the CoE's Convention.[265]

Scholars also seek justification for the separation of the two rights in the Charter. For example, De Hert and Gutwirth propose two justifications.[266] The first justification is regarding a search for a basis for the fundamental rights objective of the EU data privacy regime.[267] From inception, the EU Directive had the dual objectives of establishing the internal market and protecting fundamental rights.[268] The market integration objective has always overshadowed the fundamental rights objective.[269] As a consequence, there was a need for a legal basis for the human rights objective. The second reason advanced, which is related to the first, is that the human rights objective was less clear as the EU Directive contains more 'business friendly provisions.'[270] Lynskey rejects these justifications.[271] She argues that it is unsatisfactory to accept that a new right will be recognised to *ex post facto* legitimise an existing legislation.[272] One is tempted to go with the logic of Lynskey's

---

262 De Hert & Gutwirth (n 200 above) 8-10. Rather, art 1 which provides for the objective of the Directive merely makes reference to the right to privacy. It provides that '[i]n accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'

263 See Draft Charter of Fundamental Rights of the European Union. http://www.europarl.europa.eu/charter/pdf/04473_en.pdf (1 November 2015). The explanatory memorandum to the draft of the EU Charter has no legal value but is merely intended to clarify the provisions of the charter.

264 Lynskey (n 261 above) 570.

265 See the explanatory memorandum of the EU Charter (n 263 above).

266 De Hert & Gutwirth (n 200 above) 8.

267 De Hert & Gutwirth (n 200 above) 8.

268 European Commission 'A comprehensive approach on personal data protection in the European Union' Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM (2010) 609 final 2 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (accessed 1 November 2015).

269 De Hert & Gutwirth also noted that the commission has also conceded to this prevalence of the internal market objective. (n 200 above) 8.

270 De Hert & Gutwirth (n 200 above) 8.

271 Lynskey (n 261 above) 571.

272 Lynskey (n 261 above) 571.

argument, however, De Hert and Gutwirth's contention seems more plausible having regards to recent developments in European data privacy law. This is because the draft EU Regulation makes express reference to the EU Charter's provision on the right to data privacy. It provides in article 1(2) that '[t]his Regulation protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'[273] It may therefore be argued that, the separation of these two rights was, indeed, because of the EU's search for a basis for the fundamental rights objective of data privacy.

All the above are, however, speculative. What is clear, according to Lynskey, is that the EU is yet to justify the inclusion of both rights in its Charter.[274] Scholars have also not agreed on a proper justification. Be that as it may, both rights now exist in the EU legal order. With time, it can be expected that many more countries will also start making provisions for an independent right to data privacy so as to serve as a basis for their laws on the protection of individuals with regard to their personal information processing. The forgoing notwithstanding, an attempt will be made to establish the nature of the relationship between both rights.

2.6.1. Is the right to data privacy subsumed under the right to privacy?

Quite a number of commentators argue that the right to data privacy is subsumed under the right to privacy.[275] Others contend that both rights are interchangeable.[276] A possible reason for both contentions may be because the most influential international data privacy instruments provide that privacy is the core of data privacy.[277] Data privacy instruments in many jurisdictions also provide that realising the right to privacy is the main object of their data privacy law.[278] The courts in some of these jurisdictions refuse to apply data privacy

---

273 Draft EU Regulation (n 203 above).

274 Lynskey (n 261 above) 572.

275 R Clarke 'Introduction to dataveillance and information privacy, definitions of terms' http://www.rogerclarke.com/DV/Intro.html (accessed 1 November 2014). DJ Solove ''I've got nothing to hide' and other misunderstandings of privacy' (2007) 44 *San Diego Law Review* 754.

276 Allotey opines that '[i]nformation privacy provides individuals with certain rights over the collection, use and disclosure of their personal information. The two terms, data protection and information privacy, refer to the same privacy interest, namely a person's right of control over the storage and usage of data about him or herself. The two terms are used interchangeably in this thesis.' AKE Allotey 'Data protection and transborder data flows: Implications for Nigeria's integration into the global network economy' unpublished LL.D thesis, University of South Africa, 2014 30. See also De Hert & Gutwirth (n 200 above) 4. The authors contend that data privacy is a late "spin off".

277 Eg, art 1(1) EU Directive, art 1 CoE Convention.

278 Eg, see 2nd Paragraph of the preamble of the Protection of Personal Information Act, South Africa 2013. 'the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information'

rules in cases where there is no breach of the right to privacy.[279] The view that data privacy is subsumed under privacy also finds support in the jurisprudence of the Court of Justice of the European Union (CJEU). The decisions of the court before and after the adoption Treaty of Lisbon in 2009, which gave binding force to the EU Charter, seem to conflate both rights.[280] The European Court of Human Rights (ECtHR) adopts a similar approach.[281] This approach is debatably so because privacy has significantly influenced and played a central role to the data privacy. [282]

The data privacy laws in the jurisdictions that conflate both rights do not define privacy in relation to data privacy.[283] This failure undoubtedly reflects the notorious difficulties associated with attempts to ascribe a precise, analytical, serviceable and generally accepted meaning of privacy.[284] It therefore brings about further obscurity regarding the place of privacy in data protection law and the relationship between both rights. That notwithstanding, Bygrave argues that the failure to define privacy in data privacy laws is not a weakness as it allows for flexibility in implementation.[285] He further points out that such vagueness enables data privacy laws to 'assimilate and address a range of fears related to increasingly intrusive data processing practices'.[286]

Arguably, due to the increasingly broad spectrum within which the concept of privacy operates, it has been interpreted to cover emerging challenges with regard to personal information processing.[287] Therefore, many jurisdictions (including Canada and South

---

279 De Hert & Gutwirth (n 200 above) 32. See the UK's case of *Durant v Financial Services Authority* (2003) EWHC Civ 1746, Auld LJ at para 28. The UK Court of Appeal in interpreting the nature of personal data of a data subject held that 'it is [only] information that affects his privacy, whether in his personal or family life, business or professional capacity'

280 Lynskey (n 261 above) 575-581. See De Hert & Gutwirth's analysis of the decision of the court in *Österreichischer Rundfunk and others* (2003) ECR I-4989, (n 200 above) 29-33. Lynskey's discussion on the *Rundfunk's case* and *Productores de Música de España (Promusicae) v Telefónica de España* [2008] ECR I-271 is also shows insights. (n 261 above) 275-276. For decision of the CJEU that conflated both rights after the adoption of the Lisbon Treaty in 2009, see *European Commission v Bavarian Lager* [2010] ECR I-6055.

281 Lynskey (n 261 above) 581.

282 Bygrave (n 234 above) 281. See also Tzanou (n 261 above) 91. Indeed, Tzanou argues that 'privacy is an umbrella notion for a plurality of things that covers aspects of data protection ...'(n 261 above) 96

283 Bygrave (n 261 above) 278.

284 Bygrave (n 261 above) 278.

285 Bygrave (n 261 above) 278.

286 Bygrave (n 261 above) 278.

287 There are controversies regarding whether the concept of 'privacy' and 'respect for private and family life' mean the same thing. It is contended that the concept of 'private and family' life has a broader scope than 'privacy'. The ECtHR usually interpret private life in a wider perspective. It is on this basis that the unlawful processing of personal information may fall within the provisions of art 8 of the ECHR. See generally R Wong 'Privacy: Charting its developments and prospects' in M Klang & A

Africa) and scholars perceive data privacy as a subcategory of privacy, within the realms of 'information control' and not 'secrecy' or 'non-interference' paradigms.[288] The leading voice in this regard is Alan Westin who defines privacy in terms of information control.[289] Neethling also has a similar conception of privacy.[290] It is based on this view that most data privacy instruments provide that realising privacy is a primary objective. A problem with this conception is that there is the risk that data privacy infringements may be interpreted in the light of privacy criteria. Thus, an infringement of data privacy may only be upheld by the court if it also amounts to privacy (secrecy or confidentiality) violation.[291] The contemporary 'personal information problem' as contended by Solove, however, goes beyond mere issues of non-interference depicted by the traditional right to privacy.[292] It is therefore submitted that in as much as a regime protects information which is not, strictly speaking, private and does not subject infringements to strict privacy criteria of non-interference, it is a *sui generis* data privacy regime. This is so irrespective of the nomenclature used. Therefore the Canadian and South African regimes, even though widely perceived as subsumed under privacy, are data privacy regimes within the context of this study.[293] This is because, as will be shown later, they protect interests, beyond privacy interest.

From the forgoing, it is submitted that to flatly argue that both rights are one does no justice to the exact nature of the right to data privacy. Data privacy certainly does more in terms of personal data protection than the right to privacy. Data privacy, among others, seeks to promote interest such as autonomy, dignity, non-discrimination and liberty. It is based on this reasoning that de Andrade argues that data privacy:

Murray *Human rights in the digital age* (2005) 152. See also Fuster's discussions with regard to the jurisprudence of the ECtHR. (n 126 above) 94 & 97. See also the case of *Rotaru v Romonia* (2000) RJD 2000-V, App. No 28341/95. In this case, the ECtHR was of the view that public information can also fall within the ambit of 'private life' especially when systematically collected and stored. Page 42

288 Generally referred to as 'control-based definition.' See Wong (n 287 above) 149. Indeed, Bergelson points out that '[t]he right of information privacy is a subcategory of privacy in general, and, like the "parent" concept, it reflects the uneasy coexistence of two major competing paradigms: "privacy as secrecy" and "privacy as control."' V Bergelson 'It's personal but is it mine? Towards property rights in personal information' (2003) 37 *UC Davis Law Review* 401.

289 A Westin *Privacy and freedom* (1967) 8. See also DJ Solove 'Conceptualizing privacy' (2002) 90 *California Law Review* 1092-1126 where the learned scholar explained different dimensions of privacy in the extant literature.

290 J Neethling 'The concept of privacy in South Africa' (2005) 122(1) *The South African Law Journal* 18-28. See also Makulilo (n 261 above) 168.

291 See Lynskey (n 6 above) 76-80.

292 See generally Solove (n 58 above) 1393.

293 Based on the analysis of the meaning of data privacy in the previous chapter. See chapter 1(1.6.1).

> as such, does not directly represent any value or interest *per se*, it prescribes the procedures and methods for pursing other rights such as the right to privacy, identity, freedom of information, security, freedom of religion, etc.[294]

Accordingly, data privacy is consequently not a 'mere' sub category of the right to privacy but a very close neighbour thereto.[295] Both rights are overlapping yet distinct in other respects.[296] Both rights complement one another in protecting an individual from unlawful interference in his/her personal and private life. This distinction between both rights, according to De Hert and Papakonstantinou is, unfortunately, only recognised by the EU.[297] De Hert and Papakonstantinou further contend that the failure to recognise these differences in other parts of the world is a major impediment to the establishment of an international data privacy regime.[298] Besides, the contention that the data privacy is subsumed under the right to privacy has another downside. This is especially true with regard to developing countries, like Nigeria, with a low level of awareness on the value of data privacy protection. It may be assumed, albeit wrongly, that the constitutional or common law provisions on the right to privacy is sufficient to protect individuals from harm resulting from their data processing in this digital era. The value of a dedicated legal regime for data privacy may therefore be underestimated.

2.6.2. Problems and limitations in attempts to distinguish both rights

While it is plausible to argue that data privacy is not subsumed under the right to privacy because of its *sui generis* nature, attempts to distinguish both rights may also encounter some difficulties. For example, conceptualisation issues can be a basis for distinguishing between both rights. It can be argued that data privacy has a clear and settled definition unlike privacy. This argument is, however, problematic because it is acknowledged that trying to ascribe a particular meaning to any concept, especially legal concepts, may be a

---

294 See NN Gomes de Andrade 'Oblivion: The right to be different from oneself' (2012*) Revista de Internet, Derecho y Politica* 125. Based on this argument, the commentator concludes that 'it is…erroneous to reduce data protection to privacy.'

295 Birnhack (n 25 above) 509. Similarly, Charlesworth argues that: 'It is worth reiterating that "data protection" and "privacy" are not synonymous.' He contends further that '[d]ata protection law, in concentrating on personal data use and reuse, focuses upon aspect of privacy – informational privacy. A Charlesworth 'Understanding and managing legal issues in internet research' in N Fielding *et al The SAGE Handbook of online research methods* (2008) 44

296 Lynskey (n 261 above) 587.

297 De Hert & Papakonstantinou (n 118 above) 316.

298 De Hert & Papakonstantinou (n 118 above) 316.

practical impossibility.[299] Moreover, authors have highlighted the advantages of not having a specific definition for terms like privacy and data privacy as it provides room for the much needed flexibility in application.[300] It is therefore submitted that trying to distinguish privacy from data privacy on the basis of definitional difficulties is not without its own problems. This is so especially for a term that is associated with the constant state of flux in technology.

Another perceived difference between privacy and data privacy is that the former is prohibitive while the latter is not.[301] Privacy, unlike data privacy, prohibits the unreasonable interference into certain spheres of a person's life which is considered private and personal. It is thus a tool of opacity. Data privacy on the other hand is a tool of transparency as it affirms the permitted level of processing.[302] Thus, apart from the major interest which data privacy laws seek to foster - processing of individuals' data in a fair and lawful manner - it also promotes the interest of the data controllers in that it does not prohibit the legitimate processing of personal data.[303] Indeed, Charlesworth argues that '[d]ata protection laws are […] rarely designed, or used, to place an outright bar upon use of an individual's personal data…' Bygrave describes data privacy laws in the language of road signs, saying that 'it usually posts the warning 'Proceed with Care'; it rarely orders 'Stop!'[304]

---

299 N Tobi *Sources of Nigerian law* (1996) 103 states: 'The definition of an expression is not an easy undertaking or exercise. This is more so in legal expressions, which in most cases, do not have a precise legal meaning, and *a 'fortiori* legal definition. Every writer defines an expression for his own purpose, and in the light of his own experiences and probably his idiosyncrasies. Accordingly, a definition will certainly have that individualistic coloration.'

300 Eg, Bygrave (n 261 above) 278.

301 P De Hert & E Schreuders 'The relevance of Convention 108', 33, 42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19-20 November 2001 citied in 'EU study on the legal analysis of a single market for information society: New rules for a new age?' 4 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=833 (accessed on 1 November 2015). These scholars, however, argue that data privacy could also be prohibitive. Eg, processing of sensitive data is generally prohibited.

302 De Hert & Gutwirth (n 201 above) 77. See also Zalnieriute (n 180 above)104.

303 Charlesworth (n 295 above) 44 arguing that '[d]ata protection laws are …rarely designed, or used, to place an outright bar upon use of an individual's personal data…'

304 Bygrave (n 140 above) 122. He furthermore equates data privacy law to the principle of sustainable development in environmental law. The principles of sustainable development seek to preserve the environment but at the same time seek to promote economic growth. Data privacy too, seeks to protect the privacy interest of data subjects and at the same time promote the legitimate interests of data controllers in the processing of personal data. De Hert & Gutwirth also express similar thoughts, though, in a different context. The scholars liken data privacy with criminal law and opine that the rule of 'thou shall not kill' in criminal law is replaced with 'though can process personal data under certain circumstances'. (n 201 above) 77.

Yet, an attempt to distinguish between the rights on the basis that one is prohibitive and the other is not, is also problematic. In certain circumstance, data privacy laws, indeed, say 'stop' and prohibit the processing of personal data.[305] This is more so for personal data that is considered 'sensitive', such as data relating to race, religion, and political affiliations.[306] In addition, Makulilo contends that in specific circumstances, consent may bring about a prohibition in data privacy law.[307] One of the justifications for lawful processing is consent, however, if consent is lacking or subsequently withdrawn, processing is prohibited in the absence of another justification.[308]

The above has shown that an attempt to draw a distinction between privacy and data privacy may also face some problems. This is because both of these concepts are linked in a certain kind of way. They appear to share a parent-child relationship.[309] Data privacy seems to be an offspring of privacy and both rights are inextricably tied with a birth cord.[310] Both concepts, according to Fuster, partially overlap.[311]

2.6.3. The 'added-value' of the right to data privacy in the information society

Attempts to totally remove data privacy from the realms of privacy may be difficult, as the normative basis of data privacy law relies heavily on the right to privacy in human rights instruments.[312] Both terms are increasingly becoming synonymous and interchangeable in their daily uses.[313] Both rights also serve many of the same objectives like regulation of unauthorised surveillance and enhancing the exercising of other rights guaranteed in democratic societies.[314] This research therefore suggests that, because of the difficulties associated with trying to absolutely separate or distinguish between the two rights, a

---

305 De Hert & Gutwirth (n 200 above) 4.

306 Art 8(1) of the EU Directive. However, sensitive information could be processed under art 8(2).

307 Makulilo (n 261 above) 166.

308 There are still other difficulties in attempt to distinguish both rights. Eg, a commentator argues that data privacy is a procedural right for the effective realisation of privacy which is the substantive right. His basis for this contention is that data privacy, unlike privacy, does not uphold any particular value rather it is a means for the realisation of other values or interests. It is difficult to agree with this argument too as data privacy has its substantive dimension. See de Andrade (n 294 above) 125. See also G Zanfir 'Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law' in S Gutwirth *et al Reloading data protection: Multidisciplinary insights and contemporary challenges* (2014) 245.

309 Tzanou (n 261 above) 88.

310 Tzanou (n 261 above) 88.

311 Fuster (n 126 above) 214.

312 Such as UDHR, ECHR and ICCPR.

313 Makulilo points out that 'that the two concepts are increasingly becoming synonymous and hence interchangeable in their daily uses.' (n 261 above) 166. Lloyd also points out that 'there is a strong linkage between the notions of privacy and data protection.' (n 3 above) 30.

314 Lynskey (n 261 above) 588.

neutral approach should be adopted. Hence, attention should be directed at how the right to data privacy complements the right to privacy. Therefore, what does data privacy add to the right to privacy (what is its 'added value')?

With the rapid pace in technological development and the numerous threats personal data is increasingly being exposed to, the right to data privacy, no doubt, has an added value. It is submitted that because of its 'added value', the right to data privacy is better placed than the right to privacy to tackle the challenges of protecting individuals' personal data in the digital age and the information society.

Next the 'added value' of the right to data privacy will be considered.

2.6.3.1. Data privacy has a broader scope than the right to privacy

The right to data privacy certainly does more than the right to privacy in terms of the protection of personal data. In other words, data privacy has a wider scope than the right to privacy in the context of protection of individuals with regard to the uses of their information by entities.[315] It protects personal data which is broadly defined as any data which *reasonably* identifies a natural person.[316] This definition is wide enough to cover a large range of information relating to a person which may not be covered by the right to privacy, since the right to privacy protects personal information that is considered to be private. Not all personal information is private. Data privacy also covers a wide range of activities carried out on personal information, like the collection, storage, usage, transmission, and destruction of data. Kuner aptly notes that 'it is difficult to conceive of any operation performed on personal data in electronic commerce which is not covered by it [data privacy]'.[317]

Similarly, De Hert & Gutwirth point out that data privacy is at the same time both wider, but also more specific than the right to privacy. They contend that data privacy is wider because it relates to other fundamental rights such as equality and due process, and it is more specific in that it mainly deals with the protection of personal data. It is also broader

315 Article 29 Data Protection Working Party 'Opinion 4/2007 on the concept of personal' http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (accessed 1 November 2015) 7. See also Lynskey (n 261 above) 569.

316 Article 29 Working Party (n 315 above) 25; PM Schwartz & DJ Solove 'Reconciling personal information in the United States and European Union'(2014) 102 *California Law Review* 877-916.

317 C Kuner *European data protection law: Corporate compliance and regulation* (2007) 74.

because it protects all personal data.[318] Schartum also identifies the broader scope of data privacy in personal data protection as opposed to information privacy.[319] He points out that information privacy is a subset of the right to privacy and it essentially involves autonomy or rather 'inaccessibility' or 'opacity' of private information. However, data privacy is more of an open or transparent concept that includes information privacy but covers more than that.[320] In this light, data privacy does not only seek to make personal information confidential, but also ensures that individuals have access to their personal information in the hands of other persons to ensure it is adequate and correct it if need be. This is where the right to data privacy intersects with the right to freedom of information.[321]

2.6.3.2. Data privacy (further) enhances individuals' control of information relating to them

Data privacy complements the right to privacy by enhancing individuals' control over their personal data. The basis of the right to data privacy is informational self-determination,[322] a philosophy that holds that an individual owns his/her personal information and it is left to the individual to determine if it should be disclosed and how it should be used. Data privacy, therefore, promotes the right to informational self-determination which is an aspect of personality rights.[323] Lynskey observes that the enhanced control over personal data which the right to data privacy bestows upon individuals serves two broad purposes: it promotes individuals' personality rights which are threatened by personal data processing,

---

318 See De Hert & Gutwirth (n 200 above) 9-10.

319 DW Schartum 'Designing and formulating data protection laws' (2008) 18 *International Journal of Law and Information Technology* 2.

320 Schartum (n 319 above) 2.

321 See generally I Currie, 'The Protection of Personal Information Act and its impact on freedom of information', (2010) http://www.opendemocracy.org.za/wp-content/uploads/2010/10/The-Protection-of-Personal-Information-Act-and-its-Impact-on-Freedom-of-Information-by-Iain-Currie.pdf (accessed 1 November 2014).

322 Informational self-determination represents the substance of data privacy in Europe as expressed by the German Constitutional Court in the *census* case. It is the basis of data privacy in Germany. The German Constitution has a specific provision for the right to informational self-determination, art 2(1). Thus in Germany, the objective of the right to data privacy is to promote informational self-determination. Informational self-determination is neither mentioned in the EU Charter nor the Directive, despite the fact that it forms the essence of data privacy law. It is, however, contained in previous drafts of the Charter. Lynskey opines that its non-inclusion in the Charter may be because it 'may have been perceived by the drafters as more closely aligned to the German legal system than was appropriate in the pluralistic EU legal order.' Lynskey (n 261 above) 591; Zanfir (n 82 above) 152.

323 Lynskey (n 261 above) 569, 589.

and it also reduces informational and power asymmetries between individuals and data controllers.[324]

a. Promotes individuals' personality rights

By promoting personality rights, an individual is allowed to live his life the way he wants without the fear of being watched or monitored. The sense that a person is being monitored makes him act in a conscious manner. Thus, his/her actions are being influenced by a feeling of being watched. This affects an individual's personality right to self-development.[325] Whether or not surveillance is actually being carried out on a person is immaterial in this respect as the mere feeling of been monitored is actually sufficient to inhibit individuals' behaviour.[326] This kind of surveillance which is sought to be restricted by both privacy and data privacy rights can deter self-development by making an individual conform to certain invisible code of behaviour.[327]

With data privacy however, an individual will be able to tailor how he/she wants to be perceived by the society. In this regard, data privacy facilitates 'selective presentation' unlike the right to privacy and thereby serves as a tool to freely develop our personality.[328] It enables an individual to control what part of his personality he wants to portray to particular segment of the society. Control of personal information processing will, for example, enable a person to create a 'digital persona' in the cyberspace or internet. An individual can determine what face he/she intends to show on different platforms such as Facebook, Instagram, twitter or MySpace.

Indeed, we find that many of the rules on data processing contained in data privacy regulations are specifically tailored towards enhancing an individual's control over his/her personal data.[329] The draft EU Regulation has taken further steps to enhance this right of control of data processing. New rights which are being introduced by the Regulation, such

---

324 Lynskey (n 261 above) 569, 589.

325 See generally A Rouvroy & Y Poullet 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy' in S Gutwirth *et al* *Reinventing data protection* (2009) 53.

326 Lynskey (n 261 above) 590.

327 Lynskey (n 261 above) 588.

328 See Rodotà (n 1 above) 80, Lynskey (n 261 above) 591.

329 Neethling contends that in South African law, privacy protection in the law of delict gives an individual the right to determine when his/her personal data may be lawfully processed. However, it cannot give him/her active control. Provisions on active control are, however, needed to supplement the "traditional principles" of the law of delict for privacy protection. The active control principles can only be implemented by means of legislation, in this case, data privacy laws. Neethling *et al* (n 26 above) 334.

as the right to data portability, have been linked with enhancing information self-determination.[330] The right to data portability also has a foundation in the free development of human personality.[331]

b. Reduction in imbalance of power

The right to data privacy complements the right to privacy in reducing power and information asymmetries between individuals and data controllers.[332] By expanding the right of control over personal data, data privacy enhances the status of individuals *vis-à-vis* data controllers.[333] Data controllers are usually large organisations or the government with undue advantage over individuals in terms of power and resources. This undue advantage brings a form of asymmetry between the data controllers and individuals. Data privacy, thus, reduces these asymmetries by vesting individuals with rights over the processing of their personal data.

2.6.3.3. Data privacy serves other interests beyond privacy interests

The right to data privacy also supplements the right to privacy as it seeks to protect other interests beyond privacy related interests.[334] The right to data privacy, by promoting information self-determination, protects the dignity of an individual. Dignity is protected by ensuring that governments and businesses do not determine an individual's destiny. Data privacy also protects an individual's right to autonomy. It promotes equality and freedom in a democratic society.

Above all, the right to data privacy, like the right to privacy, prevents discrimination with the special rules on sensitive data processing and the prohibition of automated decision making or profiling,[335] data privacy prevents discrimination in that certain sensitive information, like a person's health information, is only permitted to be processed subject to stringent conditions. Also, the prohibition of automated decision making or profiling

330 See Zanfir (n 82 above) 151.
331 Zanfir (n 82 above) 151.
332 Lynskey points out that 'power asymmetries are present when one party in a relationship is in a position of strength relative to the other while information asymmetries are present when one party in a relationship is in possession of more information than another' (n 260 above) 24.
333 Lynskey (n 261 above) 593.
334 S Gutwirth & M Hildebrandt 'Some caveats on profiling' in S Gutwirth *et al* (eds) *Data protection in a profiled world* (2010) 37.
335 See art 15, EU Directive and art 20(1), draft EU Regulation. Art 15 of the Directive provides that every person has the right 'not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data.'

prevents discrimination as it precludes judgment (or decision) from being made on an individual based on traits of a similar group.[336] Such kinds of generalisations may be wrong or faulty and could lead to unfair treatment of an individual.

Data privacy also helps safeguard 'data security' and 'data quality'.[337] It safeguards data security because it ensures that data controllers put adequate security measures in place to protect personal data. A data controller is accountable for the safety and security of personal data in his/her possession.[338] This is indeed an added value of the right to data privacy. Regarding data quality, data privacy rules ensure that information is accurate, adequate, updated and relevant.[339] This serves the interest of both the data controller and the data subject.[340]

2.7. Approaches to data privacy protection

While there seems to be some level of consensus that individuals are severely threatened by the unregulated processing of their personal information, there is still a lot of controversy regarding the most appropriate legal structure to adopt in protecting personal information. The debate, in this regard, is primarily centred on the particular entity which should play a prominent role in establishing and implementing data privacy standards. It is important to state that laws on data privacy in most jurisdictions provide for essentially the same principles, since they all are largely based on the same international documents.[341] However, if one descends from the highest level of abstraction, there are significant differences in details which are influenced by the differences in the cultural, historical, and legal approaches to data privacy.[342] This is not surprising, since concepts such as 'data protection' and 'privacy' derived from national legal culture and tradition, hence they considerably vary around the world, even in systems that accept the same fundamental principles.[343] For example, the EU and Canada centrally supervise the private sector's use of personal data, whereas the regulation of the private sector in the US is reduced to the

336 Roos (n 103 above) 7 – 8.
337 Tzanou (n 261 above) 91.
338 Art 17(1).
339 Art 6 (1) (c) & (d).
340 It safeguards the interests of the data controllers in that 'it allows them to make accurate decisions based on valid, adequate and relevant data. Equally, it is in the interests of the data subjects, as inaccurate information held on them means concomitant inaccuracy in the sketching of the "digital persona" of those individuals.' See Tzanou (n 261 above) 91.
341 Kuner (n 37 above) 310.
342 Kuner (n 37 above) 310.
343 Kuner (n 37 above) 310.

barest minimum.[344] This difference in regulatory approaches is deeply rooted in differences in the conceptual basis of privacy in these jurisdictions.[345]

For the purpose of realising the right to data privacy, four main approaches, identified by scholars, have been adopted in different jurisdictions. They are the comprehensive, the sectoral and the self-regulation approaches as well as the use of Privacy by Design (PbD). Most jurisdictions' regime on data privacy, therefore, falls into one of these models. Another model which is increasingly being used, but rarely discussed, is the co-regulatory model. The strengths and weaknesses of each of these approaches will now be considered.

2.7.1. Comprehensive approach or government regulatory approach

In a comprehensive approach, the government plays the major role in the regulation of data processing activities.[346] An omnibus law which regulates the processing of personal data is enacted by the state. The law is made in such a way that it provides for very broad principles which cover all sectors of processing of personal data. The provisions of the law are enforced by a particular institutional body, usually, a public authority generically referred to as a DPA.[347] This body performs an array of functions which include enforcement, oversight, investigatory and monitoring function. The DPA in most jurisdictions that adopt the comprehensive approach is also responsible for educating and enlightening the public on various data privacy issues. The role of a DPA in a comprehensive approach is indeed crucial.[348]

The comprehensive approach is the favoured model of the EU and countries in Europe. African countries too are increasingly adopting this approach.[349] Many countries across the world with data privacy legislation also adopt this approach. The comprehensive approach

344 De Hert & Gutwirth (n 200 above) 10.

345 Eg, in the US, privacy protection is for the purposes of securing liberty especially from government. For Europeans, privacy protection is for the purpose of dignity of individuals or for protecting their public image. In Canada, privacy protection is focused on individual autonomy. See A Levin & MJ Nicholson 'Privacy law in the United States, the EU and Canada: The allure of the middle ground' (2005) 2 *University of Ottawa Law & Technology Journal* 357–395. See also De Hert & Gutwirth (n 200 above) 10.

346 It is also called government or command and control model. See Allotey (n 276 above) 380.

347 The enforcement body is termed differently in different jurisdictions: Commissioner, Ombudsman or Registrar. It must be pointed out that the Data Protection Authorities are not the only enforcement bodies of the right to data privacy. Other bodies like the like the tribunals and courts play a significant role in enforcement. See Privacy International 'Privacy and human rights: An international survey of privacy laws and practice' http://gilc.org/privacy/survey/intro.html (accessed 1 November 2015).

348 See 'A comprehensive approach on personal data protection in the European Union' (n 348 above).

349 African countries with a comprehensive approach to data privacy include Ghana, Kenya, Cape Verde and most recently, South Africa.

is a preferred model for countries without an existing system for data privacy protection.[350] It is preferred because enforceability is higher in this model. The approach is also more effective in countries that adhere to a system of general law and governmental oversight.[351]

The general law in the comprehensive model adopts a 'one size fits all' approach whereby the law regulates data processing both in the private and public sectors. It is, however, flexible enough in that it allows for development of sectoral codes to regulate particular sectors that carry out highly sensitive data processing activities.[352]

Proponents of this approach strongly support government overarching control of the private sector processing of personal data because the desire for profit and the economic value attached to personal data 'will prevent firms from taking adequate steps to protect personal data'.[353] Governments' control in this regard, will provide the much needed strong grip in regulating private entities.[354] Moreover, this approach provides for a coherent and harmonised system of regulation of data processing. This may serve as an effective tool for realising effective protection data privacy.

Despite the perceived advantages of this approach, it has come under increasing criticism.[355] The major argument against the model is the 'one size fits all' approach used to regulate the processing of personal data. The approach seems impracticable, as providing for a broad range of processing activities that cover different sectors in a single legislation may be quite complicated. Moreover, advances in technology which bring about new challenges to data privacy may not be anticipated and provided for by a comprehensive omnibus law. This will mean amending such a law at regular intervals with the attendant cumbersome processes in amendments of laws and cost associated therewith. Another argument against this approach is that too much emphasis is placed on the law in

350 Privacy International (n 348 above); Moshell (n 48 above) 366.

351 Moshell (n 48 above) 366.

352 For eg, recital 61 of the EU Directive provides that: '[w]hereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation.'
Also compare Recital 68 which provides that '[w]hereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles.'

353 Allotey (n 276 above) 380; see also CJ Bennett & CD Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (2003)134.

354 Allotey (n 276 above) 380.

355 See Bergkamp (n 34 above) 31- 47; Koops (n 206 above) 8.

books as against the law in practice. This means there is an absolute disconnect between the laws as provided in books and as it operates in practice.[356] Furthermore, the model is said to inhibit innovation, involves a high cost to implement, is inflexible and gives diminishing returns.[357]

2.7.2. Self-regulatory approach or industry/market approach

Those who criticise government's stronghold on personal data processing activities argue that a self-regulatory approach may yield better results.[358] In this approach, private entities, companies and industries establish regulatory mechanisms through codes and self-policing.[359] The government plays a very limited role in the regulation of data processing activities.[360] The self-regulatory/market approach is subdivided into two types. The first is the *laissez-faire* approach which leaves a particular business to determine its data privacy policies.[361] The market also influences data privacy practices. The second is the self-regulatory approach which enables a group of businesses to come together and develop a data privacy code which shall be binding on them all.[362] This can be effectively done through their professional or trade associations.

The self-regulatory approach may be mistaken to be the same with absence of regulation because of the minimal state influence. However, this is not the case. In the self-regulatory approach, binding codes are established by businesses which provide for minimum standards for data processing practices. In some cases, the standards which are provided usually incorporate the fair information principles (FIPs) or are a reflection of them.[363]

Proponents of this approach argue that businesses will shape their policies according to consumer preferences as economic success depends on increasing market share by attracting customers.[364] Businesses will enhance their competitive positions by responding to consumers preferences for greater privacy, thereby leading to a more privacy friendly

---

356 Koops (n 206 above) 8.
357 Allotey (n 276 above) 380.
358 Allotey (n 276 above) 381.
359 Privacy International (n 347 above); Moshell (n 48 above) 367.
360 J Strauss & KS Rogerson 'Policies for online privacy in the United States and the European Union' (2002) 19 *Telematics and Informatics* 179.
361 Strauss & Rogerson (n 360 above) 179.
362 Strauss & Rogerson (n 360 above) 179.
363 Eg, the Canadian Standard Association (CSA) which was later incorporated in the Canadian Personal Information Protection and Electronic Document Act (PIPEDA).
364 Strauss & Rogerson (n 360 above) 179.

web.[365] Based on this argument, businesses will be in the best position to know their customers' needs with regard to data privacy and will make adjustments based on customers' demands. This is so as to enhance their competitive positions in the market. The argument is that a customer will leave a particular business for another one if he/she is not satisfied with their data privacy protection policies. In this case, the market will device means to arrive at an optimal level of privacy protection.

This regulatory approach has a strong support base in the US because of the view that government's influence in the private sector will suppress the growth of businesses. Indeed, it has been stated that 'for electronic commerce to flourish, the private sector must continue to lead'.[366] Consequently, innovations will arise in a market driven arena not in an environment regulated by the government.[367] Thus, 'governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organisations to develop mechanisms to facilitate the successful operation of the internet.'[368] The relative support gained in the US is due to the fact that processing of personal data raises serious economic and business issues which the US government typically hands-off from, so as to allow for free and fair competition among businesses and thereby encourage growth.

The main advantage of this approach is its maximum flexibility.[369] Industries in a particular sector are in a better position to determine when and how to regulate personal data processing.[370] This may inevitably lead to higher levels of voluntary compliance as industry participants are more likely to comply with rules developed by their peers than outside bodies such as government agencies.[371] Other advantages of this approach include efficiency and reduced cost.[372]

The increased incentive for compliance advantage, may, however, be exaggerated. The absence of strict sanctions for violation of industry codes will make business entities

365 Hirsch (n 20 above) 455.
366 See 'Framework for global electronic commerce' http://www.w3.org/TR/NOTE-framework-970706 (accessed 1 November 2015).
367 Framework for global electronic commerce (n 366 above).
368 Framework for global electronic commerce (n 366 above).
369 Strauss & Rogerson (n 360 above) 179.
370 See Allotey (n 276 above) 382.
371 Rowland *et al* (n 95 above) 16.
372 Allotey (n 276 above) 384.

continue to violate individuals' rights to data privacy.[373] This is due to their desire to maximise profit at all cost. They, therefore, either go unpunished or pay small fines which may just be a meagre sum compared to the huge profit realised from data processing and trading. Moreover, the effectiveness of an approach totally devoid of government influence, in realising the right to data privacy is doubtful. Government is the institution that grants rights to the people. They also wield the necessary power or authority to ensure that the rights granted to the people are enforced. Examples of this approach are rare because countries, especially the US, have been disappointed with efforts based on self-regulation.[374]

2.7.3. Co-regulatory approach or hybrid approach

The numerous arguments against too much governmental control over data processing and the apparent weaknesses of a total lack of governmental influence have led to a 'middle-ground' or a 'hybrid' approach.[375] This is an approach in which both the industry and the government play complementary roles in data privacy protection - that is a co-regulatory approach.[376] The approach is neither a pure government regulation approach, nor is it a pure industry self-regulation approach, but rather a hybrid of both.[377] Both the government and private entities share the responsibilities of setting and enforcing regulatory goals and standards.[378] They may do so by splitting tasks.[379] The co-regulatory approach is 'not a new phenomenon and can be found at various places in the regulatory landscape.'[380]

Some of the arguments in support of this approach are that, it provides the 'best of both worlds' as there is an enforceable rigorous approach that protects data privacy while also keeping up with, and meeting the needs of, the growing internet economy.[381] A co-regulatory approach is also flexible as it allows the industry to play an active role in setting data privacy standards. Like the self-regulatory approach, flexibility is an advantage in a co-regulatory model, because industry members have a unique knowledge of their

---

373 Allotey (n 276 above) 384.
374 Privacy International (n 347 above); Moshell (n 48 above) 367.
375 Hirsch (n 20 above) 440.
376 Data Security Council of India 'Strengthening data protection through co-regulation' available at http://cis-india.org/internet-governance/blog/strengthening-privacy-protection.pdf (accessed 1 November 2015). See also Hirsch (n 20 above) 441.
377 Hirsch (n 20 above) 441.
378 Hirsch (n 20 above) 465.
379 Hirsch (n 20 above) 465.
380 Hirsch (n 20 above) 441.
381 Hirsch (n 20 above) 441.

businesses and strategies.[382] It is also argued on behalf of a co-regulatory approach that 'it provides the flexibility of self-regulation while adding the supervision and rigour of government rules.'[383]

The approach is not without its critics as noted by Hirsch.[384] Some commentaries have stated that the approach lacks transparency and accountability.[385] It has also been stated that an agreement between the government and the industry to share regulatory functions will most likely produce deals that will tilt in favour of the industry thereby setting-aside public interest.[386]

This approach is being used by countries like Canada and Australia.[387] With regard to the EU, it is debatable if it also provides for a co-regulatory approach to data privacy regulation. It is generally known that the EU adopts a comprehensive approach. This fact has been reiterated by scholars.[388] Several documents emanating from the EU have also stated the fact of its comprehensive regime.[389] However, certain provisions in the EU Directive point to something different.[390] Article 27 for example, provides that:

> The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

These codes developed by group of industries in the private sector are to be submitted to the national authorities for approval.[391] This provision therefore shows that a co-regulatory regime is anticipated by the EU. However, as pointed out by Bygrave, nothing provided in

382 See Hirsch (n 20 above) 465-466 for more on the strengths of this approach.
383 See Hirsch (n 20 above) 441.
384 See Hirsch (n 20 above) 441.
385 Hirsch (n 20 above) 441.
386 Hirsch (n 20 above) 441.
387 'Comparing the co-regulatory model, comprehensive laws and the sectoral approach' available at https://www.cippguide.org/2010/06/01/comparing-the-co-regulatory-model-comprehensive-laws-and-the-sectoral-approach/ (accessed 1 November 2015). Privacy International (n 347 above); Moshell (n 48 above) 366.
388 Eg, Lloyd (n 3 above) 26.
389 See, eg, 'A comprehensive approach on personal data protection in the European Union' (n 348 above).
390 See also recital 61 & 68 of the EU Directive.
391 Art 27 (2); Some authors have described this type of regime as 'enforced self-regulation' or 'regulated self-regulation' see Rowland *et al* (n 95 above) 19.

article 27 shows the exact legal status of such codes.[392] This provision has still not been clarified by the EU.[393] Scholars therefore contend that it is an on-going debate.[394]

2.7.4. Sectoral approach

This model of regulation of data privacy is very close to the comprehensive approach. What distinguishes both approaches is the overarching law which covers all sectors of data privacy. In the sectoral approach, there is no general law which regulates all sectors of data processing. Rather, laws are enacted to target all those specific industries or sectors which pose the greatest threat to data privacy.[395] Like the comprehensive approach, the government also plays a prominent role in the regulation of processing activities.

The main advantage of this approach is that laws are enacted to cater for specific sectors based on the unique threat the sector poses to data privacy protection. As a consequence, such laws will be narrow enough to provide for personal data protection based on practices in a specific sector. Moreover, it may be argued that industries in a specific sector will have more influence in the making of such sectoral laws. This approach can be very effective when complementing the comprehensive approach. It has, however, also been argued that when used alone, the sectoral approach results in ineffective enforcement and excessive legislative lag time.[396] Further criticism of the sectoral approach is that enforcement under this model is inconsistent due to the lack of a central enforcement agency or DPA.[397]

The regulation of data privacy in the US is predominantly sectoral in nature.[398] Most data privacy laws are only enacted to cover a particular sector.[399] This 'patchwork quilt' system

---

392 Bygrave (n 183 above) 36.

393 The exact status of codes that are "ascertained" to be in accordance with the relevant national law is left somewhat open: The Directive does not require that the assessment amounts to a formal "approval" of such codes or that they be given any formal status within the legal systems of the Member States, and national practice varies. See European Commission 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments' JLS/2008/C4/011 – 30-CE-0219363/00-28 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1636706 (accessed 1 November 2015).

394 Hirsch (n 20 above) 479.

395 Privacy International (n 347 above); Moshell (n 48 above) 367.

396 Privacy International (n 347 above).

397 Privacy International (n 347 above).

398 Lloyd (n 3 above) 26. See also De Terwange (168 note) 179.

399 Eg, Cable Communications Policy Act of 1984, Video Privacy Protection Act of 1988, Fair Credit Reporting Act of 1970 and Gramm-Leach –Bliley Act of 1999. See RW London 'Comparative Data Protection and Security Law: A Critical Evaluation of Legal Standards' unpublished LL.D thesis, University of South Africa, 2013 433.

of laws regulating data privacy has come under intense criticism especially by European scholars.[400]

2.7.5. Privacy by design (PbD)

A relatively new approach to data privacy regulation is the use of PbD. PbD was a concept promoted by Ann Cavoukian in the 1990s (the former Information and Privacy Commissioner of Ontario, Canada). The idea has become widespread, although as an aspirational tool rather than a concept with legal force.[401] This approach entails embedding data privacy principles into the design of technology. It is a proactive rather than a reactive approach as it neither waits for privacy risk to materialise nor does it offer remedies for resolving privacy infractions once they have occurred.[402] Some jurisdictions, like the UK, have been advocating for the acceptance of this approach.[403] Likewise, PbD is becoming a legal and regulatory requirement around the world.[404] The approach is said to be generally good. However, it is still largely based on 'recommendations' without having the force of law. Moreover, Bernal points out that it places more emphasis on encouraging the flow of data rather than individual rights.[405]

From the above, it is clear that all the approaches have their individual strengths and weaknesses. It is therefore contended that in most instances, those approaches that are the most effective combine several aspects of the different approaches.[406]

2.8. Other mechanisms in data privacy protection: An appraisal of Lessig's theory

The recent complexities in the nature and form of data processing activities have made personal data increasingly vulnerable. These complexities have also shown that the task of

400 Privacy International (n 347 above); Moshell (n 42 above) 367

401 Bernal (n 240 above) 257.

402 '7 foundational principles' http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/ (accessed 1 November 2015).

403 See Bernal (n 240 above) 257 thesis. See also 'Privacy by design' http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design (accessed 1 November 2015).

404 See art. 17, EU Directive & art 23, draft EU Regulation for provisions relating to 'data protection by design or default'. See also A Cavoukian 'Privacy by Design: Leadership, methods, and results' in S. Gutwirth *et al European data protection: Coming of age* (2013) 175.

405 Bernal (n 240 above) 258.

406 See OECD Ministerial Declaration on the Protection of Privacy on Global Networks Privacy International 'A borderless world: Realising the potential of global electronic commerce' 7-9 October 1998. http://www.oecd.org/internet/ieconomy/1840065.pdf (accessed 1 November 2015). See also Privacy International (n 347 above); Moshell (n 48 above) 366.

protecting personal data in the face of new and emerging 'privacy destroying technologies' could be overwhelming. Consequently, effective regulation of data processing may equally be overwhelming for pure legal instruments. This is not to undermine the power of the law in regulating conduct within a society. However, legal instruments also have their own limitations. Expressing concerns regarding the difficulty in adequately protecting data privacy, the European Commission points out that:

> We fear that there is no "magic bullet" to ensure adequate data protection. The law is by its nature often difficult to interpret and apply, and either too vague or too inflexible, while supplementary and alternative (non-legal or quasi-legal) measures have suffered from serious, often inherent weaknesses.[407]

The above concern shows that effective data privacy regulation may only be achieved by collaborative efforts between the law and other non-legal instruments. Some theories could therefore be applied in data privacy regulation. Notable among the theories is that of Lawrence Lessig, which is expounded in his book *Code 2.0*. Though, the theory is not specifically on regulation of data privacy, Lessig's ideas has aspects which could benefit debates on effective regulation of data privacy.[408]

The thrust of Lessig's theory is centred on the way in which human behaviour on the internet, or more specifically, cyberspace, can be effectively regulated. Lessig rejects the general contention that the cyberspace cannot be regulated because of the difficulties of establishing government presence in it. He contends that, cyberspace, contrary to the prevailing argument, is capable of being regulated effectively. This is by the use of what he calls the code. The code essentially entails making the architecture or design of the internet or cyberspace to be controllable or capable of being regulated. In this regard, emphasis is therefore placed on the technology of a particular facility on the internet which should be designed in such a way as to ensure effective control. The predominance of threats to data privacy protection is found on the internet or more appropriately, in cyberspace. Lessig's theory, therefore finds relevance in regards to data privacy.

Lessig explains the four main factors or modalities that can be effectively used to ensure privacy on the internet or cyberspace. These instruments are the law, norms, market and

---

407 European Commission (n 393 above).

408 Moreover, some authors argue that Lessig's theory is simple and applicable beyond the technological realm which perhaps explains its popular success. Rowland *et al* (n 95 above) 7.

architecture/code.[409] These factors or modalities will help ensure control of cyberspace. In relation to data privacy regulation, these instruments will ensure that individuals are able to control their personal data on the internet and make choices with regard to who may use them and how they should be used. This is, indeed, the crux of the *sui generis* right to data privacy.

2.8.1. Law

Lessig acknowledges legal instruments as the first means of regulation of data privacy. Such law can be divided into three types viz: substantive, procedural and enabling law.[410] Most of the discussion in this chapter focuses on the laws regulating data privacy, hence laws will not be considered in detail here. What is important to note is that such laws should be clearly drafted so as to foreclose any form of speculations on its provisions which may hinder its application in response to data privacy threats.[411] It is also submitted that a viable institutional body to complement the law in enforcements of data privacy principles is also imperative. The role of the judicial arm of government in interpreting and upholding the law is also vital.[412]

2.8.2. Norms

Norms are the standard patterns of behaviour that is considered as normal in a given society. There are various ways in which norms can be influenced to achieve certain desired conduct. For example, norms among businesses that process personal data could help build certain privacy protection practices.[413] Another way norms can be influenced to regulate personal data processing is by educating and enlightening the public on the dangers associated with the processing of personal data. This means they also have a role to play by ensuring that their personal data is not arbitrarily disclosed on social media and the internet.[414]

---

409 Lessig (n 30 above) 223.
410 Lessig (n 30 above) 227.
411 Lessig (n 30 above) 223. Lessig states that the law should come out expressly to prohibit unlawful or unfair data processing practices.
412 Lessig (n 30 above) 124. See also V Mayer-Schönberger 'Demystifying Lessig' (2008) *Wisconsin Law Review* 716.
413 Lessig (n 30 above) 223.
414 Allen (n 33 above) 845.

2.8.3. Market

The government can also use the market to regulate data processing in cyberspace. This can be done by many instrumentalities. The government can influence a rise in the prices of devices for processing activities. It could also heavily tax companies that process personal data so as to discourage processing. The government could provide incentives to enable more competition among service providers on the internet. As regards data privacy, websites that collect personal data should be able to compete among each other. Thus, if a user is not comfortable with the data privacy practices of a particular service provider, he/she can easily move to another service provider. This serves another function of edging out service providers with poor data protection policies.

2.8.4. Architecture/code

Architecture or code is yet another very useful tool in the regulation of data privacy. Code/architecture within the context of Lessig's model is the design or make of a particular technology for processing personal data such as a computer or internet. In other words, code/architecture is the use of technology to regulate data processing. Our information and communication technologies can be designed in almost any way we want, Lessig states.[415] They are much more plastic or open to change than most other technologies we use.[416] Technology (code/architecture) may be used by the government to regulate/protect data privacy.[417] Such technology that enhances data privacy is called privacy enhancing technologies (PETs). PETs are technologies which enable individuals to have more technical control over their personal information in cyberspace.[418] These technologies are usually integrated into the design/architecture of an internet facility like a website. For example, websites could be designed in such a way that the collection of personal data is made impossible, or extremely limited. A website may also be designed so as to enable users know that their personal data will be collected and why it is collected. This will give users an element of choice to decide whether to use such a website and have their personal data collected, or leave the said website and have their personal data preserved.

---

415 Lessig (n 30 above) 32.
416 Lessig (n 30 above) 32. See also Mayer-Schönberger (n 412 above) 717.
417 Lessig (n 30 above) 32
418 Lessig (n 30 above) 223.

PETs, in addition, have functions to enable users determine the amount of their data that is given out or used for other purposes. For example, a social networking site may be designed in such a way as to allow a user to adjust the privacy settings for their own purposes. This gives them an element of choice in determining what data is revealed about them. Examples of PETs, as explained by Lessig, include the 'identity layer' and a protocol called platform for privacy preferences (P3P). The introduction of an 'identity layer' enables individuals more effective control over what data about them is revealed. It would also allow users to have trusted pseudonymous identities that websites and others can trust. Thus, with this type of technology, if a site wants to know certain information about a user, like age, or authorisation to access certain facility, it can obtain these data without knowing anything else about the user.[419]

P3P[420] on the other hand is a protocol[421] that enables websites to state the purpose of collection of users' personal data in a standard format that can be retrieved automatically and interpreted easily by user agents.[422] A user agent (usually web browsers) is a software that acts on behalf of a user when he/she is navigating the internet which helps in understanding cryptic commands.[423] P3P user agents will allow users to be informed of the website practices (in both machine and human-readable formats)[424] and to automate decision-making based on these practices when appropriate. [425] Thus, P3P provides a means for an individual to recognise when a site does not comply with his/her privacy preferences.[426] This is a very important PET as users do not need to read the privacy policies every time they visit a site. Moreover, users hardly read these policies as they are

419 Lessig (n 30 above) 226.

420 The Platform for Privacy Preferences Project (P3P) enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit. 'Platform for Privacy Preferences (P3P) Project' http://www.w3.org/P3P/ (accessed 1 November 2015).

421 A protocol is 'a set of rules that controls the way data is sent between computers'. See Oxford advanced learners dictionaries. http://www.oxforddictionaries.com/definition/learner/protocol (accessed 1 November 2015).

422 P3P (n 420 above).

423 The internet is actually completely text-based thus to browse, one needs to type certain text commands. However, with the development of user agent, there was no more need for an internet user to understand cryptic commands as a user agent does that on behalf an internet user. In many cases, a web browser such as Firefox, chrome, internet explorer is usually used as a user agent. See 'What's my user agent' http://whatsmyuseragent.com/WhatsAUserAgent (accessed 1 November 2015).

424 It is not every data or file a computer can understand and interpret. Only files in machine readable formats may be are accepted by the computer. Thus, machine readable format is presenting a file in a form that is understandable and acceptable to the computer.

425 P3P (n 420 above).

426 P3P (n 420 above).

usually in a technical and complicated manner and bulky in most cases. The P3P will recognise and immediately flag a website that is privacy intrusive. A user will, therefore, be left with the choice to determine whether or not to proceed. In many circumstances, a web browser will give a user notice such as 'site not trusted due to privacy settings' or 'cookies are enabled' and may not allow a user proceed because of that. These are the effects of P3P.

In the context of IT, code or architecture comes to the forefront of regulatory debate because the whole regulatory domain is man-made hence, easily manipulated by public and private actors.[427] Thus, Lessig is less interested in laws, norms and market and concentrates more on the power of architecture as an effective tool to regulate the cyberspace.[428]

Regarding law/legal instruments particularly, Lessig downplays their importance as effective regulator of the cyberspace. This is because laws are usually enacted through highly formalised and complex democratic mechanisms.[429] It is difficult, expensive and time consuming to pass a law.[430] Moreover, it takes a very long process for laws to come into force as they have to be made public and scrutinised.[431] A code on the other hand is much cheaper and faster to create.[432] It is built into the software that we use. It does not need to be made transparent and is devoid of cumbersome legislative processes and debates. All that is necessary is for the engineers in a corporation producing the software, to code it.[433] Another scholar, Bergkamp, also supports the use of architecture/code in data privacy protection. He states that technological advances such as privacy-preference procedures and blocking and filtering software will enhance privacy since individuals will have access to most of the technologies needed to obtain the level of privacy protection desired.[434]

427 Rowland *et al* (n 95 above)8
428 Lessig (n 30 above) 123. See also Mayer-Schönberger (n 412 above) 716.
429 Lessig (n 20 above) 72. Mayer-Schönberger (n 412 above) 717.
430 Mayer-Schönberger (n 412 above) 717.
431 Mayer-Schönberger (n 412 above) 717.
432 Mayer-Schönberger(n 412 above)717.
433 Mayer-Schönberger(n 412 above)717.
434 Bergkamp (n 34 above) 37.

2.8.5. Lessig's central argument on effective regulation of personal information processing

The thrust of Lessig's theory in relation to data privacy is that regulation of the cyberspace and privacy related issues can only be done through a combination of one or more of the above tools (that is law, norms, market or code). In his words, 'there is no single solution to policy problems on the internet. Every solution requires a mix of at least two modalities.'[435] This is the Lessig's 'optimal mix' proposition. The particular two that will be adopted is dependent on the nature of the data privacy threat. Lessig refrained from making a prescriptive argument for the particular two to be adopted. He points out that: 'I don't insist on the particular solutions I propose, but I do insist that solutions in the context of cyberspace are the product of such a mix'.[436] Consequently, for a particular data privacy threat, the law and codes or the law and the market could be influenced to ensure adequate protection of data privacy.

Despite Lessig's recommendations of alternatives to legal regulations, it is observed that the law plays a predominant role in influencing all the other models. Legal regulation forms the platform on which each of the other regulatory tools operates. The law defines the substance of data privacy and provides the limits of processing of personal data. Moreover, it is the government who seek a change or want to exercise control over each of the regulatory tools described above. Apart from the fact that government is an establishment of the law, it influences change mainly by policies and laws. This shows that the role of legal instruments cannot be downplayed. However, for effective legal regulation, other mechanisms may also be used. Despite the relative success in explaining power relations in cyberspace, some scholars have criticised the Lessig's theory.[437]

---

435 Lessig (n 30 above) 223.

436 Lessig (n 30 above) 224.

437 Eg, Mayer-Schönberger has criticised there role Lessig ascribes to market as a means for regulating the cyberspaces. See V Mayer-Schönberger (n 412 above) 713-746. Similarly Gutwirth contends that Lessig's argument is not relevant for the legal profession that practices law because regulation is too wide a concept to accommodate the specificity of legal practice and emerging technologies. See S Gutwirth *et al* "The trouble with technology regulation from a legal perspective. Why Lessig's 'optimal mix' will not work" in Brownsword R & Yeung K *Regulating technologies* (2008) 193-218.

2.9. Criticisms of the *sui generis* right to data privacy: An evaluation of the major arguments

Proponents of the right to data privacy continue to argue for its increasing relevance in the information age and digital society. It is said that it enables people to act autonomously thereby strengthening democracy; it enables people to decide what face they want others to see, which allows self-development etc.[438] This notwithstanding, there are numerous criticisms against the *sui generis* right to the protection of data privacy.[439] Arguably, the foundation of these criticisms is the suggestion that 'privacy is dead' in the information society and 'we should learn to get over it'.[440] There are still other argument against regulation of personal data processing and the whole data privacy regime inspired by the EU system. Most of the criticisms come for US scholars who have a totally different approach to data privacy regulation.[441] Some of these criticisms will be considered.

2.9.1. Data privacy has no significance if you have 'nothing to hide'

It has been suggested that protection of (data) privacy is outmoded.[442] After all, if you have nothing to hide, you need not worry about privacy.[443] In this regard, it is common for people to argue that they are not bothered when the government collects or analyses their personal data.[444] This is because 'only if you are doing something wrong should you worry, and then you don't deserve to keep it private.'[445] This statement shows that people are ready to give up their privacy interest for safety and security purposes.[446] The

438 Fromholz (n 196 above) 465.

439 Most of the criticisms are with regard to the EU data privacy regime. However, it is still relevant in this part because the majority of data privacy regimes are largely tailored in line with the EU regime. For more on the criticisms, see Bergkamp (n 34 above) 31-47; Koops (n 206 above).

440 Steve Rambam is the founder and CEO of Pallorium Inc., a licensed Investigative agency. In a keynote speech, he was of the opinion that privacy no longer exists in this age. He states that 'privacy is dead - get over it' https://www.youtube.com/playlist?list=PL8C71542205AA51E5 (accessed 1 November 2015). Also in 1999, Scott McNealy, the Chief Executive of Sun Microsystems, stated that 'you have zero privacy. Get over it' http://www.afr.com/p/national/no_such_thing_as_privacy_on_the_-UjYlyyDX2vc7M2nGVI132M (accessed 1 November 2015).

441 I have considered their arguments in the self-regulatory approach.

442 A statement credited to Mark Zuckerberg, CEO of Facebook. See Craig & Ludloff (n 11 above) 9.

443 Solove (n 275 above) 748.

444 DJ Solove "Why Privacy Matters Even if You Have 'Nothing to Hide'" http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/ (Accessed 1 November 2015).

445 Solove opines that this argument is not of recent vintage as one of the characters in Henry James's 1888 novel, *The Reverberator*, states that 'if these people had done bad things, they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing.' See Solove (n 444 above) 749.

446 Solove (n 444 above).

argument, though directed at privacy generally, is relevant in a discourse on data privacy as it was earlier pointed out that data privacy and privacy relate in diverse ways (2.6).

Proponents of the nothing-to-hide thesis argue that the government can accumulate as much information as possible for the purposes of safety and security of the people. This argument raises certain issues bordering on the value of the right to data privacy. Three of these arguments will be considered. First, is the particular entity that collects the personal data. Secondly, they type of personal data collected and thirdly, the purpose for which the data is to be used. Regarding the first, it has been established that even though the government is a large data controller, private individuals also engage in the massive collection of individuals' personal data. Moreover, with internet and IT, information sharing between the government and private individuals is being carried out on a larger scale. It may thus be assumed that the government is collecting personal data for security purposes when, in actual fact, such data is being collected by private entities for commercial purposes. The law on data privacy protects individuals from misuse of such personal information.

Secondly, the nothing-to-hide argument will have some merit if the type of data being collected is known. Rarely will anyone know the kind of information being gathered about him/her as such will not be publicly disclosed.[447] One may therefore assume that the data being collected regarding him/her is strictly for the purpose of ensuring his/her security or safety when in essence, other personal information is being collected such as information on religious and political views or race. Related to this is the purpose for which the data collected is used.[448] Even if it is the government that collects this personal information, is it being used for the purposes for which it is collected? Is it indeed being collected for security purposes? In the past, such questions may not have arisen because data was used mostly for a single purpose.[449] Today, in the new economy and in a public sector ready for e-government, data is used for several purposes and much more intensely and effectively than ever before.[450] For example, personal data collected for security purposes, may be used by another government department to determine if a person should be entitled to

447 Solove (n 444 above).
448 Solove calls this the problem of 'exclusion'. He defines exclusion in this respect as occurring when people are prevented from having knowledge about how information about them is being used and where they are barred from accessing and correcting errors in the data. Solove (n 444 above).
449 De Hert and Gutwirth (n 200 above).
450 De Hert and Gutwirth (n 200 above).

certain social benefits. This exposes individuals' personal data to abuse or misuse. Use of individuals' personal data for purposes other than that which they are collected exposes individuals to huge risks, some of which include profiling and discrimination. Craig and Ludloff replied to the 'nothing to hide' argument in very apt words that '… if you make that statement to anyone who has been racially or religiously profiled, you might be surprised at his reaction.'[451]

The 'nothing to hide' argument also undermines the dignitary interest which data privacy seeks to protect. Amongst the several interests which data privacy seeks to protect is the right to personal dignity. A person should be a free moral agent to determine whether personal data about him/her should be collected and how it should be used. The seamless collection of individuals' personal data takes away his/her right to dignity and deprives him/her of the power of informational self-determination. Some entities (either government or private) have some form of power over individuals which is vested by the control of their personal data.

The advocates of the nothing-to-hide argument therefore undermine the importance of the right to data privacy. They tend to look at the issue of data privacy from the point of view of collection of data rather than the use of such data. They also assume that collection of information is a 'once off' thing when what they should be really bothered about is the accumulation of tiny bits of sensitive information about individuals. This argument considers data privacy in the information society within a very narrow perspective. According to Solove:

> The nothing-to-hide argument focuses on just one or two particular kinds of privacy problems - the disclosure of personal information or surveillance - while ignoring the others. It assumes a particular view about what privacy entails, to the exclusion of other perspectives.[452]

It is thus submitted that the 'nothing-to-hide' argument is based on misleading assumptions about (data) privacy and its value in the contemporary society.

---

451 Craig & Ludloff (n 11 above) 9.
452 Solove (n 444 above).

2.9.2. Too much focus on informational self-determination is unrealistic

It has been argued that data privacy regime inspired by the EU focuses too much on informational self-determination which may be unrealistic in the digital age. Though data privacy and informational self-determination are not synonymous, the latter is without doubt at the heart of the former. According to Koops, informational self-determination is the notion that people should be able to exercise control over what happens to their personal data, after all, it is theirs.[453] The most feasible way individuals can exercise informational self-determination is by requiring their consent to process their personal data. Koop therefore argues that the right to informational self-determination is unrealistic for three reasons.[454] The first is that obtaining consent is a myth as it is 'largely theoretical and has no practical meaning'.[455] This is because with internet based services, people seldom read or understand the privacy statements and they just tick consent boxes while service providers assume users are informed of privacy policies. Moreover, consent to processing can be valid only if there is an alternative. He argues that 'often, there is little to choose: if you want to use a service, you have to comply with the conditions, if you do not tick the consent box, access will be denied'[456]

The second reason advanced as to why the right to informational self-determination is unrealistic, is that the exercise of control over personal data, whether or not based on consent, 'is extremely difficult, if not impossible, for individuals to realise in the 21st century data-processing practices'.[457] This is because of the complexities of present day data processing activities involving multiple data controllers which are usually unknown to the data subjects. In many cases, data subjects do not know if and what data on them is being processed by a data controller. Moreover, data controllers rarely comply with data privacy laws.

The third reason advanced is that, even if informational self-determination theoretically functions in private relationships, it will rarely function in citizen/government relations. This is because 'citizens exercising control over what happens with their personal data… is

453 Koops (n 206 above) 251.
454 Solove (n 444 above).
455 Solove (n 444 above).
456 Koops (n 206 above) 252.
457 Koops (n 206 above) 251.

at odds with the character of the public sector.'[458] In most cases, data processing in the public sector relies on legal obligations or public interest as a justification for the data processing and not on a citizen's consent to the processing.

The arguments advanced by Koops as to the unrealistic nature of informational self-determination in data privacy regimes, have some merit because of the complex dimension in modern day data processing activities. However, it must be pointed out that some of these concerns appear to have been considered by the EU regime and efforts are being made to tackle these challenges so as to enhance control over the personal data by individuals. The draft EU Regulation grants individuals certain rights, which strengthens their control over personal data. Some of these rights are the right to data portability and right to be forgotten.[459] Moreover, more emphasis is being placed on the use of technologies to regulate data processing activities[460] so as to enhance the power of control by the data subject. Regarding the difficulty to control data processing by the government, one finds it hard to agree with the Koops' argument as his fears seem to have been exaggerated. Data processing activities of the government could be put in check by DPAs. This is why it is recommended that the functions of the DPA should be exercised by an autonomous body, independent from the government.[461]

2.9.3. Data privacy negatively affects commerce and market

It is contented that because information is essential to the market based economy which depends critically on accessibility of data, its processing should not be regulated.[462] This is because the free flow of information has increased productivity and the efficiency of production.[463] Moreover, use of personal data facilitates targeted advertising and direct marketing. This also benefits consumers as they receive better services at cheaper prices. Regulation of personal data processing limits their choices and makes them receive out-

458 Koops (n 206 above) 251.
459 Koops (n 206 above) 251.
460 By the use of PET and privacy-by-design instrumentalities.
461 See recital 62 and art 28 of the EU Directive. See also G Greenleaf 'Independence of data privacy authorities (Part I): International standards' (2012) 28 *Computer & Security Review* 3-13. G Greenleaf 'Independence of data privacy authorities: International standards and Asia-Pacific experience' (2012) 28 *Computer & Security Review.*
462 Bergkamp (n 33 above) 34.
463 Art 20(1), EU Directive.

dated information on products and services. Furthermore, it is contended that data privacy restricts competition and thereby negatively affects the market.[464]

The contention that data privacy affects commerce is also misdirected. The argument portrays data privacy as absolutely prohibiting the processing of personal data which is not the case. Data privacy is not prohibitive; it does not forbid the processing of personal data. It merely lays down rules for the lawful processing of personal data to enable individuals to have more confidence that their personal information is secure. In this way, it fosters trade and commerce as it enhances the trust of users in the businesses being transacted.[465]

2.9.4. Data privacy brings about misrepresentation and fraud

Another criticism of the right to data privacy is that it brings about fraud.[466] This is because informational self-determination, which is at the heart of the right to data privacy, allows an individual to determine what face he wants to present to the people. Berkgamp argues that 'by allowing people to determine the face they want to present to the world, we allow them to deprive others of a competitive or economic advantage, or to improve their own position otherwise at the expense of others.'[467] Thus, data privacy denies others from knowing the 'not so good' side of individuals and to communicate it to others which brings about fraud and misrepresentation.

In rejecting this criticism, it must be pointed out that data privacy provides rules for data quality.[468] This is to ensure that the information being processed is accurate, adequate and up to date. It enables accurate assessment of a person to be made based on the quality of the relevant data. It therefore means that an individual cannot misrepresent as decisions are made based on accurate and updated data.

2.9.5. Data privacy restricts freedom of information/speech

Bergkamp contends that data privacy regime, especially the EU style, has the effect of affecting other fundamental rights like freedom of information and speech. 'Securing one person's privacy may infringe on another person's freedom of expression and

464 Bergkamp (n 34 above) 39.
465 Birnhack (n 25 above) 510.
466 Bergkamp (n 34 above) 36.
467 Bergkamp (n 34 above) 36
468 EU Directive, art 6(1)(c).

information'.[469] As a consequence, it is contended that the government has no business regulating data privacy. Without doubt, data privacy regime may have the effect of restricting another person's right to freedom of information. However, it must be stated that even freedom of information principles restrict access to personal data of other persons. This is a general exception to freedom of information (FOI) which the right to data privacy strengthens.

Data privacy also complements freedom of information in another way. A person cannot approach a public body for access to his/her own personal data under Freedom of Information (FOI) Act. Such right can, however, be exercised through the general principles of data privacy.[470] A provision in the EU Directive, for example, grants an individual access to information in the hands of a data controller.[471] Data privacy also complements freedom of information and protects other persons' right by restricting access to personal data regarding other persons.[472] The EU style data privacy laws also grant an exception for the processing of personal data for artistic journalistic and literary purposes.[473] In this regard, the legal protection of data privacy does not restrict freedom of speech and the press but rather supports it. From the above, the argument that data privacy restricts freedom of information and speech is misconceived.

The discussion above shows that a data privacy regime is necessary. However, a proper balance should be struck between an individual's interest in privacy and other conflicting interests such as safety and security, free flow of personal information, freedom of information and speech and so on. Thus, an effective data privacy regime must balance these competing and sometimes conflicting demands.

2.10. Chapter conclusion

This chapter has two broad objectives. The first is to demonstrate the fact that data privacy is a very serious issue which ought to attract the attention of policymakers and scholars in any jurisdiction in the world. The second objective of the chapter is to show the development of data privacy law under international law. These two objectives are very

469 Bergkamp (n 34 above) 35
470 EU Directive, recital 72.
471 EU Directive, recital 41, art 12.
472 EU Directive, recital 42.
473 See EU Directive, recital 37.

crucial at this stage of Nigeria's development, especially with respect to information technology. Advances in technology naturally come with challenges which an effective legal system must be proactive in confronting. Unregulated processing of individuals' information threatens human rights and fundamental freedoms which every democratic society ought to take seriously. Therefore, the chapter first established the significance of personal data in the digital society. The nature of the threats to personal data in the information society was also discussed. In this regard, it was argued that various means aided by advances in technology are used to exploit personal data because of its significance today. Some of the data privacy intrusive means with associated risk were examined. An attempt was made to show the global nature of data processing activities which is not restricted to only advanced countries. Implicitly, it was argued that data privacy challenges affect all countries, irrespective their level of advance in technology hence, the concerted global responses.

Therefore, the chapter considered the emergence and development of the *sui generis* right to data privacy as a response to the challenges of modern-day data processing. Various instruments at the international level with significant contribution to the jurisprudence on the law of data privacy were discussed. However, the initial contribution of some countries at the national level was briefly noted. It was also observed that regional instruments, especially in Europe and Asia significantly contributed to the law on data privacy. Nevertheless, the same cannot be said of Africa who has remained dormant in the field until recently with the adoption of the AU Convention on Data Protection. The contribution of human rights instruments also was noted.

A vexed issue on the development of data privacy is its status as a human right. This has generated so much debate. The thrust of the debate regarding data privacy as either a human right or an issue of commerce was considered. It was submitted that, although data privacy in its origin and development has commercial affiliations, its status as a human right cannot be denied. As a human right, another contested issue on the development of data privacy is its relationship (and/or difference) with the right to privacy. Here, it was argued that an attempt to totally remove data privacy from privacy will be difficult. Thus, it was suggested that rather than attempt a watertight distinction between both rights, the 'added-value' of a right to data privacy should be the focus of the discussion.

Though the law on data privacy is based on similar principles, various jurisdictions have approach the protection of data privacy in different ways. Thus, the strengths and weaknesses of the diverse regulatory models were examined. This is a foundation to subsequent discussions on a proposed legal framework for Nigeria. The sophistication of contemporary data processing activities has exposed the weaknesses of the law. Lessig therefore propounded a theory for effective protection of personal data with a particular focus on the internet. He proposed other regulatory mechanisms. This theory is also useful for a proposed framework for data privacy in Nigeria.

Finally, an attempt was made to consider some of the common arguments against the right to data privacy. Despite the numerous criticisms concerning the need for the right to data privacy, its utility in this era of big data and digital devices cannot be taken too lightly. It must therefore be adequately protected using appropriate mechanisms. However, protection of data privacy has to contend with other competing and equally important values such as security of life and property and commercial interests of other individuals. This makes data privacy a very controversial issue in this digital society. Indeed, the European Consumer Commissioner notes that issues of data privacy is 'one of the most important and controversial issues in the fast evolving world of digital communications.'[474] Due to the sweeping wave of globalisation, every country ought to consider it as a pressing issue and key into the overwhelming debate on data privacy. In this light, the next chapter considers the state of data privacy protection in Nigeria.

[474] Kuvena (n 4 above).

Chapter three

The legal framework for the protection of data privacy in Nigeria: Issues and challenges

3.1. Introduction

> *If data were nuclear particles or perhaps even genetically modified foodstuffs, people would be aware of and respectful of the dangers involved in their use and transportation. The danger today is that data flows are invisible and when society becomes aware of their potential for misuse, it may be too late to put this technological genie back in the bottle.*[1]

The previous chapter showed the importance of personal data in the information society and threats individuals are being exposed to as a result of its processing. It was argued that data privacy is generating much debate at various fora, hence no country should be left out of such debates. Most importantly, data privacy is currently raising substantial issues of human rights which every country must take very seriously. Building on these facts, this chapter examines the state of data privacy protection in Nigeria. This is done by analysing various challenges at different levels which stand in the way of the effective realisation of the right to data privacy in Nigeria.

Nigeria is a developing economy with a very large population.[2] It is also a growing market for various products and services. Nigeria plays a very vital role economically and

1 IJ Lloyd *Information technology law* (2014) 25.

2 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 figures change nothing as Nigeria's economic output is underperforming. See

politically in the West African region specifically and Africa in general. It also arguably claims the position of 'giant of Africa.' Nigeria is fast becoming a big information market with a significant rise in exposure to information and communication technologies (ICTs). Its vast population makes the personal information of the people a very vital resource. These reasons and many more make Nigeria attract significant attention regionally and globally. It also raises questions regarding what legal mechanisms are in place to protect individuals' personal information.

This chapter therefore analyses the legal framework for the protection of data privacy and the challenges to the effective realisation of this right in Nigeria. Investigation into this issue is crucial because it may be assumed that because of the significant attention the country attracts and the fact that it plays a leading role in Africa, issues of data privacy protection will be taken seriously. Such assumptions may yield false conclusions. As a prelude to discussions on the legal framework for data privacy protection in Nigeria, however, certain vital issues will be considered.

The Nigerian society has significantly changed in terms of information technology (IT) with the advances in technology. The extent of such change may be underrated by an ordinary observer. As a consequence, a brief description of the ICT landscape today will be carried out in part 3.2, with a view to showing how Nigeria has transformed within the last few years in terms of ICT development. These transformations, as will be argued, have advertently or inadvertently created numerous legal issues. One such issue created by transformation in ICT in Nigeria is the nature and extent of data processing. It is usually asserted by scholars and policymakers that ICT is not so advanced as to enable large-scale processing of personal data in the country. Hence, it is argued that, Nigerians need not be bothered about protection of their personal data and ultimately, their right to data privacy. This chapter, in part 3.3, sets the record straight by providing an insight into the current trend in personal data processing and explaining why Nigerians need to worry. Based on the nature of personal data processing, parts 3.4 and 3.5 analyse the extant (and prospective) legal and institutional framework for the protection of data privacy. Analysis of the legal regime will be carried out with a view to identifying existing regulations

'Nigeria becomes Africa's biggest economy' *BBC News Business* 6 April 2014, available at http://www.bbc.com/news/business-26913497 (accessed 1 November 2015).

(binding and non-binding) that protect data privacy and evaluating how effective they are in realising the right to data privacy.

Part 3.6 of this chapter examines the various draft bills on data privacy protection in Nigeria so as to predict their efficacy in the event that any one of them is eventually enacted as law. In this way, the chapter updates the existing literature on data privacy law in the country. Another addition the chapter makes to the existing literature in part 3.7, is a consideration of the regional and sub-regional instruments on data privacy and how they have influenced (or how they will influence) the effective protection of data privacy in Nigeria. This is particularly crucial in the wake of the recent African Union (AU) Convention on Cyber-security and Personal Data Protection (2014).

Several practical challenges stand in the way of realising adequate protection of personal data in Nigeria. This chapter, in part 3.9, examines some of these challenges and how they impede the growth of data privacy protection in Nigeria. The chapter finally draws conclusions on the present state (and future) of data privacy protection in Nigeria and gives some insights into the next chapter.

3.2. The Nigerian society in the digital age

A discussion on issues regarding data privacy protection can only be meaningful when situated within the context of the level of ICT[3] exposure in a particular society. This is because the greater the level of exposure of a society to ICT, the greater the challenges to data privacy. The Nigeria of today is no longer the Nigeria of years ago in terms of ICT penetration.[4] Recent statistics vindicate this fact. Not too long ago, statistics had shown that the level of internet penetration[5] in Nigeria was around fifty-one percent (51%) with

---

3 ICT is an umbrella term usually used to denote communication devices or applications such as television, radio cellular phones, computer network and the internet as well as various services associated with them. See 'ICT (Information and communication technology – technologies)' http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies (accessed 1 November 2015). This section will focus on the internet and mobile phone technology because they are major features of a digital society.

4 Some authors point out that technology use has generally increased rapidly among many large developing countries like Nigeria. See MD Chinn & RW Fairlie 'ICT use in the developing world: An analysis of differences in computer and internet penetration' Working paper, National Bureau of Economic Research (July 2006) 6 also available at http://www.nber.org/papers/w12382.pdf (accessed 1 November 2015).

5 Internet penetration is 'the portion of the population that has access to the internet. It defines a portion of the digital divide.' MJ Ahn & J McNutt 'If we build it will they come? An appreciation of the microfoundations of e-government' in C Dolićanin *et al Handbook of research on democratic strategies and citizen-centered e-government service* (2015) 55.

about ninety (90) million internet users.[6] Nigeria's user growth rate for the year 2014 was about sixteen percent (16%) with an estimated ten (10) million new users that year.[7] As of July 2014, Nigeria was ranked eighth (8th) of countries with the most internet users in the world.[8] This is a significant leap from about ten (10) years ago when Nigeria was ranked twentieth (20th) in the world.[9] Nigeria is also recording a strong presence in online activities such as social networking.[10]

In a related development, there is a significant commitment by the government towards improving Nigeria's broadband access[11] as indicated by her broadband vision.[12] As rightly acknowledged by the Nigerian government, 'broadband is to the 21st century information age what electricity was to the industrial age.'[13] Statistics on the telecommunications sector, which is an integral component of ICT, has also shown massive improvement within the last few years. As of August 2015, the total number of active mobile telephone lines was estimated to be close to a hundred and fifty-two (152) million, which is about ninety percent (90%) penetration, as against less than one percent (1%) in 2000.[14]

---

6 Internet Live Stat 'Internet Usage Statistics for Africa' http://www.internetworldstats.com/stats1.htm#africa (accessed 1 December 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 1 December 2015). There are inconsistencies in figures by both sources, however, the difference is not substantial.

7 Internet live stat (n 6 above).

8 Ranked after countries like China, United States (US), India, Japan, Brazil, Russia and Germany who are classified 1st -7th respectively.

9 Internet live stat (n 6 above).

10 It has one of the highest numbers of Facebook users in Africa. See Internet Live Stat 'Africa' http://www.internetworldstats.com/africa.htm (accessed 1 November 2015).

11 The term 'broadband' 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.' 'Nigeria's National Broadband Plan 2013-2018' a submission by the presidential committee on broadband 12 available at http://www.researchictafrica.net/countries/nigeria/Nigeria_National_Broadband_Plan_2013-2018.pdf (accessed 1 November 2015) 12.

12 'The broadband vision for Nigeria is one of a society of connected communities with high speed internet and broadband access that facilitate faster socioeconomic advancement of the nation and its people.' 'Nigeria's National Broadband Plan 2013-2018' (n 11 above) 26.

13 'Nigeria's National Broadband Plan 2013-2018' (n 11 above) 13. Though broadband penetration in Nigeria is presently between 4-6%, which is very low. It has been 'empirically proven that every 10% increase in broadband penetration in developing countries results in a commensurate increase of 1.3% in GDP.' This is why the Nigerian government is committed to improving broadband penetration.

14 See 'Subscriber statistics: Monthly subscriber data' Nigerian Communications Commission http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&Itemid=73 (accessed 1 November 2015).

On various other fronts in Nigeria, the story is the same. There is a growing presence of ICT. The government for its part, is gradually adopting electronic government (e-government)[15] in many of its activities such as registration of voters and services delivery in sectors like health and education. Nigerians are gradually embracing internet banking and a total cashless (or cash-lite) policy.[16] Many establishments have moved their businesses to the online environment.[17] All of these indicate that Nigeria can now key into policy and academic debates on data privacy protection in the digital age and information society. It also shows that issues such as challenges to personal data autonomy should no longer be foreign in the present-day Nigeria.

3.3. Contemporary issues on data processing in Nigeria: Challenges for the right to data privacy

The statistics and figures given above representing Nigeria's expanding presence in the digital environment are not without some consequences. Personal data in this era of big data is available everywhere and of course, easily accessible. Issues will certainly arise from the proliferation of personal information. This section of the chapter analyses major challenges to data privacy in contemporary Nigeria. It must, however, be pointed out that the challenges considered here are not exhaustive. Rather, an attempt is made to show the most recent issues and to refute the arguments of some scholars who contend that data processing activity is low and therefore data privacy protection is not a topical issue in Nigeria today.[18] For the purpose of the discussions here, data processing activities will be

---

15 E-government is a way the government uses technologies to provide the people with convenient access to government services and information; to improve quality of services and to provide greater opportunities to participate in democratic processes and institutions. There are several recent e-government initiatives in Nigeria at the federal and state levels. At the federal level, the Nigerian Immigration Service (NIS) has adopted online payment for passports and other services. Salaries of federal government staff are also currently paid online via internet banking. The Lagos state government has also initiated e-taxation policies across the state. See A Kazeem 'Legal aspects of e-payment in government' http://www.nigerianlawguru.com/articles/general/LEGAL%20ASPECTS%20OF%20E-PAYMENT%20IN%20GOVERNMENT.pdf (accessed 1 November 2015).

16 See PC Obute 'ICT laws in Nigeria: Planning and regulating a societal journey into the future' (2014) 17(1) *Potchefstroom Electronic Law Journal* 440. See also 'Trend report: Information technology in Nigeria' (2012) *African Journal of Economics* available at http://africanjoe.com/?p=1 (accessed 1 November 2015).

17 See National Information Technology Development Agency (NITDA) Draft Guidelines on Data Protection available at http://www.nitda.gov.ng/download/dataProtection.pdf (accessed 1 November 2015).

18 A Kusamotu 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by Article 25 of European Union Directive 95/46' (2007) 16(2) *Information & Communications Technology Law* 157. His contention is that 'with such a low level of PC penetration and data processing activities within large segments of the population in Nigeria, the reasons for a

categorised into two broad groups, that is, the processing of personal data by public data controllers (or users) and the processing of data by private data controllers (or users).

3.3.1. Public data controllers

Public data controllers within the context of the discussions here are government and its numerous departments and agencies who process individuals' personal information. The data processing activities of the government that will be discussed here are data collection and use by the Nigerian Communications Commission (NCC), the Independent National Electoral Commission (INEC), the Nigeria Identity Management Commission (NIMC) and personal data processing by security agencies. Data processing of these bodies provoke the major debate on data privacy in Nigeria today.

3.3.1.1. Nigerian Communications Commission's (NCC) SIM card registration exercise

The NCC in 2010 introduced a compulsory registration scheme for users of the subscriber identity module (SIM) cards in Nigeria.[19] The scheme was adopted so as to create a credible database to ease identification of criminals as a result of concerns from security agencies.[20] Subscribers' personal information such as facial photograph and other biometric data (like fingerprints) were collected.[21] Subscribers were also required to present identification documents such as e-passports, company ID cards with tax/pension numbers, student ID cards from recognised institutions and drivers' licenses. The SIM card registration was made compulsory for all subscribers as unregistered SIM cards were to be disconnected from the networks.[22]

The fact that a large amount of personal information is collected by automated means and accumulated in a database raises issues of data privacy protection. The security of personal data in such a database is a major concern. Poor data security measures will definitely bring about cases of data breaches or mishandling of data. For example, it was reported

---

general lack of concern about the absence of EU-style data protection laws should be immediately apparent.' Apparently, the comment of the learned author was made as far back as 2007 – this could be a plausible reason for his contention.

19 Obutte (n 16 above) 438.

20 See Nigerian Communications Commission (NCC) 'SIM registration' http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=122&Itemid=113 (accessed 1 November 2015).

21 CE Izuogu 'Data protection and other implications in the ongoing SIM card registration process' http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665 (accessed 1 November 2015).

22 NCC (n 20 above).

that a laptop was missing with about one thousand (1000) users' biometric data believed to have gone with it.[23] The limitation on the use of accumulated personal data strictly for purposes for which it is collected is another concern. Unfortunately, many subscribers seem to be ignorant of the value of their personal data.[24]

3.3.1.2. Independent National Electoral Commission's (INEC) voters registration exercise and the Permanent Voter Card (PVC)

Based on its mandate as the primary electoral body in Nigeria, INEC collects personal data of individuals.[25] Personal information like voters' names, addresses and biometric data is collected for the purpose of voter registration and stored in INEC's database using computers and Direct Data Capturing (DDC) machines.[26] A PVC[27] is subsequently issued which contains these details and which enables a citizen to vote if his/her personal data matches what is stored in INEC's database. In the wake of the 2015 general elections in Nigeria, there were accusations that a political party intends to hack (or actually hacked) into INEC's database to steal voters' personal data for the purpose of rigging elections.[28] The Nigerian Chief Electoral Officer, while not ruling out the possibility of hacking in absolute terms, refuted the allegations. However, he was quick to point out that if hacking happens, there must be insider collaboration.[29] Whether or not these allegations are well-founded is not important for this discussion. What is important is the concerns arising from

---

23 J Oguntimehin 'Implications of Nigeria's National ID card' http://www.iafrikan.com/2014/09/30/nigeria-national-id-card/#sthash.aDBRkrnA.dpuf (accessed 1 November 2015).

24 AS Adeniyi 'The need for data protection law in Nigeria' https://adeadeniyi.wordpress.com/2012/07/18/the-need-for-data-protection-law-in-nigeria-2/ (accessed 1 November 2015).

25 Sec 153 (1); 3rd schedule part 1, Constitution of Federal Republic of Nigeria 1999 ('the Constitution'). See also 'About INEC' http://www.inecnigeria.org/?page_id=14 (accessed 1 November 2015).

26 DDC machines are devices used to collect personal data of voters in the registration process. The main information it collects is photographs and finger prints of voters. A DDC is used to prevent multiple voter registration and to remove ghost voters by looking for duplicates of the fingerprints recorded in the registration process. See Human Rights Watch (HRW) 'The role of the Independent National Electoral Commission (INEC)' http://www.hrw.org/legacy/backgrounder/africa/nigeria0407/5.htm (accessed 1 November 2015).

27 A PVC is a smartcard based voter ID which stores voters' personal information such as biometrics and facial image which can be used for identification and authentication of voters during elections. See INEC Revised Guidelines for Permanent Voter Card Distribution (2014) available at http://www.inecnigeria.org/wp-content/uploads/2014/02/GUILDLINES-FOR-PVC-DISTRIBUTION-FOR-COMMISSION.pdf (accessed 1 November 2015).

28 'INEC's database is fortified and cannot be hacked – Jega' http://whatsupnaija.info/inecs-database-is-fortified-and-cannot-be-hacked-jega/ (accessed 1 November 2015).

29 'Nobody can hack into INEC database - Jega' *Punch Newspaper* January 21 2015 also available at http://www.punchng.com/news/nobody-can-hack-into-inec-database-jega/ (accessed 1 November 2015).

a weak accountability and security safeguard policy of any institution that collects such sensitive personal information.

3.3.1.3. Nigeria Identity Management Commission's (NIMC) National Identity Card Scheme

The Nigerian President recently launched a new e-ID (electronic identity) card which doubles as a national ID card and an automated teller machine (ATM) card.[30] The card is to be used for identification and electronic signature (e-signature) purposes. Implementation of the project was to be in phases.[31] This scheme elicited mixed reactions from commentators. The project has been lauded for preventing data from being collected by different bodies at the same time as it is a unified biometric database.[32] Nevertheless, certain issues with regard to the scheme have provoked negative reaction from commentators. The first, as usual, is the security of sensitive personal data accumulated in a large database.[33] The second, which is more worrisome, is the collaboration with America's MasterCard, a 'foreign private firm', for the purposes of executing the project.[34] The practical implication of this partnership is that sensitive information of Nigerians (including biometric data) will be transferred to an American entity for processing.[35] It has been stated that such will 'spell doom for Nigeria's territorial integrity, as well as compromise our security as a people…'[36] This is more so in an age of massive data surveillance by the US (United States) National Security Agency (NSA).[37]

---

30 T Olagunju 'Mr President and the National Assembly: Data protection for Nigerians first' http://saharareporters.com/2014/09/02/mr-president-and-national-assembly-data-protection-nigerians-first (accessed 1 November 2015).

31 About 13 million Nigerian were to be issued the card in the first phase and an estimated 100 million for the second phase.

32 Oguntimehin (n 23 above).

33 The Director General of the NIMC said the Commission presently has the infrastructure with a capacity to store over 150 million units of identities and can also duplicate 100 million units which can enrol the entire Nigerian population. O Ezigbo 'Nigeria: Bill to Safeguard Personal Information Underway' *Thisday Newspaper* 24 February 2013. Available online in http://allafrica.com/stories/201302240286.html (accessed 1 November 2015).

34 The project actually brought together different bodies like the NIMC, MasterCard, Unified Payment Services Limited (payments processor), Cryptovision, and pilot issuing banks including Access Bank Plc. See Oguntimehin (n 23 above)

35 Oguntimehin (n 23 above),though it has been argued that MasterCard only grants access to enable payments and are not directly responsible for the biometric data on the card.

36 The MasterCard Logo will be visibly displayed on the Nigerian National Identity Card. Olagunju (n 30 above).

37 Olagunju (n 30 above).

3.3.1.4. Collection of personal data by security agencies

With the spate of insecurity and terrorist activities in Nigeria, it has been reported that the government has expanded its surveillance activities.[38] Indeed, data can constitute a valuable investigative tool, albeit with high potentials for misuse.[39] The legal issues arising from data processing activities by the security agencies of the state will not yield any fruitful academic debate because of the significant exceptions granted to them by various legislation.[40] The state hides behind these exceptions to process the personal data of its citizen (and foreigners). Gwagwa *et al*, however, point out that 'it is not acceptable to use national security concerns as a blanket justification to excuse unwarranted privacy breaches.'[41] Thus certain issues arise for academic discussion within these narrow confines. The first concerns accountability for accumulated personal data. Related to this, is safeguard of personal data in the possession of these agencies. The crucial question is: are there extra measures put in place to ensure that personal data in possession of these security agencies is protected from unscrupulous persons and businesses? This is important because of the sensitive nature of most of the accumulated information. The quality and accuracy of personal data in their possession also raises questions. Do these agencies take steps to ensure that personal data in their possession is up-to-date, accurate and not misleading? A suspect, for example, may be wrongly detained because of inaccurate or misleading personal information. It is difficult to answer these questions because the activities of security agencies are generally shrouded in secrecy. Yet, a number of concerns arise from these activities.

---

38 Eg, in 2013 there were great suspicion of internet surveillance by the government which was confirmed when it was reported that the federal government had awarded a secret contract to Israel-based Elbit Systems to help monitor internet communications in Nigeria 'under the guise of intelligence gathering and national security.' See O Emmanuel 'EXCLUSIVE: Jonathan awards $40 Million contract to Israeli company to monitor computer, internet communication by Nigerians' *Premium Times* 25 April 2013. Available at http://bit.ly/12K1rUR (accessed 1 November 2015).

39 Lloyd (n 1 above) 24.

40 Quite a number of laws grant security agencies in Nigeria powers to process personal data for law enforcement and security purposes. Eg, the Nigerian Constitution provides for the right to privacy (which includes privacy of information) which can be taken away by a law that is reasonably justifiable in a democratic society in the interest of defence and public safety (sec 45). See also sec Nigerian Cybercrime Act 2014, sec 21 & 22. Available at http://www.nassnig.org/nass/legislation.php?id=2064 (accessed 1 November 2015).

41 A Gwagwa *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 1 November 2015).

3.3.2. Private data controllers

The activities of private data controllers seem to constitute a greater challenge to data privacy in Nigeria because, unlike the public data controllers, they do not have direct legal instruments which establish them and regulate their activities; hence it will be difficult to hold them accountable. Profit making is their primary goal and this is sometimes in conflict with individuals' right to data privacy. Some contemporary manifestations of this conflict in Nigeria are considered below.

3.3.2.1. Banking Sector: BVN and KYC schemes

The proliferation of ICT in the banking sector will always come with legal issues which the law must contend with.[42] Banks and other financial institutions, through their numerous activities, accumulate large amounts of personal data. Quite recently, the Central Bank of Nigeria (CBN), in collaboration with the Bankers Committee, launched the Bank Verification Number (BVN) project as a key component of the know-your-customers (KYC) policy of the banks.[43] This project is in a bid to curb fraud in the financial sector.[44] Hence, all bank customers must be issued a unique identity (BVN) which can be verified across the banking industry. The exercise involves the collection of personal data, including photographs and other biometric data. This is a compulsory exercise which must be carried out by banks and there are substantial penalties for a bank that fails to comply.[45] Though one of the benefits of the BVN is to protect customers' bank accounts from unauthorised access, it raises data privacy concerns.

Banks in Nigeria also carry out KYC functions at regular intervals. KYC is a process used by banks to identify and get more acquainted with their customers. Personal data of customers are therefore updated regularly through this process. The risk of banks using

---

42 See generally TI Akomolede 'Contemporary legal issues in electronic commerce in Nigeria' (2008) 3 *Potchefstroom Electronic Law Journal* 17-18.

43 B Udo 'CBN sets new deadline for bank customer's verification' *Premium Times* http://www.premiumtimesng.com/business/169879-cbn-sets-new-deadline-for-bank-customers-verification.html (accessed 1 November 2015).

44 'Central Bank of Nigeria introduces Bank Verification Number (BVN)' http://nairabrains.com/2014/10/central-bank-of-nigeria-introduces-bank-verification-number-bvn/ (accessed 1 November 2015).

45 Eg, suspension of services on a customer's account. The CBN has also directed banks to honour transactions from N100 million and above, only from customers with BVN from March 2015. The directive is contained in the CBN's 'Circular on the acceleration of bank verification number (BVN) project' available at http://www.cenbank.org/Out/2014/BPSD/CIRCULAR%20ON%20ACCELERATION%20ON%20BVN2.pdf (accessed 1 November 2015).

information accumulated from the KYC and BVN processes for other purposes is very high. In some circumstances, this information can be sold to retailers or direct marketers for the purpose of advertising. Banks also make use of this information for their own purposes. For example, they advertise and directly market their own services and products. This could be in the form of unsolicited spam messages or junk mails.[46]

3.3.2.2. Telecommunications industry

Service providers in the telecommunication industry in Nigeria are potential violators of individuals' right to data privacy. They keep extensive records of personal details and communications of customers. Records of call data are retained for a very long period of time. Telecom service providers assist security agencies with call data to help prevent and investigate crimes. However, this could be abused as security agencies approach service providers for call data without the necessary warrants or permits. This is a challenge to data privacy in Nigeria.

Similarly, telecom service providers use personal details of customers for commercial purposes in two instances. Firstly, they sell this data to commercial agencies and other entities for advertising and other purposes. For example, it was reported that some politicians allegedly lobbied telecom companies for subscribers' data so as to send campaign messages.[47] Secondly, telecom service providers use accumulated personal data for their own advertisement purposes. They overrun individuals' phones with unsolicited text messages at any time of the day. This is prevalent in Nigeria.

3.3.2.3. Credit Bureaus

Credit bureaus[48] are salient private data controllers in Nigeria.[49] They collect credit information on individuals and establishments such as their credit standing, credit

---

46 Unsolicited or junk mails are mails sent out by direct marketing or direct mail firms. They are used mainly to introduce prospective customers to new products and services. 'Junk mail' http://www.businessdictionary.com/definition/junk-mail.html#ixzz3QhTdUAmC (accessed 1 November 2015).

47 B Olaleye 'Is Data Protection Act inconsequential?' http://www.gbooza.com/group/nigeriapolitics/forum/topics/is-data-protection-act#ixzz3ITCPwCy3 (accessed 1 November 2015).

48 A Credit Bureau is 'an institution that collects information from creditors and available public sources on borrower's credit history.' Central Bank of Nigeria (CBN) Guidelines for the Licensing, Operations and Regulation of Credit Bureaus in Nigeria 2007. http://www.cenbank.org/OUT/CIRCULARS/BSD/2008/GUIDELINE%20FOR%20LICENSING%20CREDIT%20BUREAU%20IN%20NIGERIA.PDF (accessed 20 January 2015).

repayments, court judgements and bankruptcies and then create a comprehensive credit record.[50] This information is sold to financial institutions that offer credit facilities - decisions on the creditworthiness of a person are taken based on that information. Currently, there are three major credit bureaus in Nigeria.[51] These bureaus have great capacity to gather vast amounts of personal data through enhanced data matching software capable of processing millions of updates per day.[52] They also possess data storage systems capable of storing millions of records.[53] And they can deploy a multi-million dollar specialised ICT infrastructure to perform their functions.[54]

Recently, there was a collaborative effort by the Credit Bureau Association of Nigeria (CBAN), the NIMC and the CBN to introduce 'unique identifiers' to ease the identification of borrowers (data subjects).[55] Definitely, several issues of concern to data privacy advocates will arise from these activities of credit bureaus. Questions such as accountability, access to update and rectify personal data will naturally arise. But the most worrisome seems to be security safeguard of personal data in the databases of these credit bureaus. As seen previously, most of the information collected is of a sensitive nature. Data processing activities of credit bureaus are so important that some countries specifically set out specific provisions regulating their activities in their data privacy laws.[56]

3.3.2.4. Retail outlets: Direct marketing

Retail outlets also collect personal data of customers. Customers' details are collected so that they can benefit from new products and services. In other cases, the gradual shift to a cashless society has made customers make purchases with their credit and debit cards. This process allows retail outlets to keep records of individuals' shopping habits and ultimately

---

49 LA Abdulrauf 'Do we need to bother about protecting our personal data?: Reflections on neglecting data protection in Nigeria' (2014) 5 *Yonsei Law Journal* 82.

50 See the CBN Guidelines (n 48 above).

51 The CRC Credit Bureau Limited, CR Services Credit Bureau Plc. and XDS Credit Bureau Limited.

52 This information is collected from several sources including commercial banks, retailers, telecom service providers, federal government enterprises & microfinance banks, finance houses, discount houses, merchant banks and leasing companies. See XDS Credit Bureau. http://www.xdscreditbureau.com/ (accessed 1 November 2015).

53 XDS Credit Bureau 'Our products and services' http://www.xdscreditbureau.com/product&services.php (accessed 1 November 2015).

54 XDS Credit Bureau (n 53 above).

55 See 'Credit Bureau Association of Nigeria' http://www.mfw4a.org/news/news-details/article/2869/credit-bureau-association-of-nigeria.html (accessed 1 November 2015).

56 Eg, Ghanaian Data Protection Act 2012, sec 36.

of their personal data. All these information is used for direct marketing purposes. Furthermore, most retail outlets in Nigeria have surveillance technology devices with capabilities to retain data for a very long period of time. This is a data privacy infringement which ultimately affects dignity and autonomy of individuals.

With many more emerging issues which pose threats to individuals, an important question is, what legal framework protects data privacy in Nigeria? This will now be considered in some detail.

3.4. The legal regime of data privacy in Nigeria: Issues and challenges

The common belief is that a country without an omnibus legislation on data privacy has no form of protection of personal data.[57] This view may be misleading as it undermines the existing constitutional and statutory provisions that may protect personal data. Thus, certain general and sectoral laws may, even though limited, have the effect of protecting individuals' from threats resulting from their data processing. Moreover, there have been strong arguments in support of the fact that the adequacy of a data privacy regime is not fully dependent on the existence or otherwise of omnibus data privacy legislation.[58] Besides, Makulilo maintains that one of the reasons for the slow growth of data privacy literature in Africa is that African writers assume that a country without a comprehensive data privacy framework will not yield quality academic discussion.[59] Hence, they[60] engage in 'pseudo comparative' study without a critical analysis of the 'anatomy of the entire system' of a data privacy legal framework in a particular jurisdiction, albeit without a comprehensive law.[61] Makulilo further explains that these African scholars are under the

---

57 This belief is held because the general trend nowadays is to protect data privacy through an omnibus legislation. Nevertheless, countries like the US do not have omnibus data privacy legislation and personal data receives protection in one form or the other in the country.

58 Blume contends that comprehensive legislation is not a mandatory requirement for a regime to be adequate as a satisfactory level of protection can be achieved through self-regulation. He, however, was quick to point out the difficulties in enforcement of rules in a self-regulatory system. P Blume ' Transborder data flow: Is there a solution in sight' (2000) 8(1) *International Data Privacy Law* 69

59 AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) *International Data Privacy Law* 176

60 Referring to African academics in the field of data privacy law.

61 Makulilo notes this in relation to a work Ubena John titled 'Privacy: A forgotten right in Tanzania' (2012) *Tanzania Lawyer* 72-114. He (Makulilo) contends that 'it is surprising in an article that has 42 pages (72 -114), that reference to Tanzania is restricted to a total space of just four pages. One would have expected to find the anatomy of the entire system of privacy in Tanzania albeit without comprehensive data privacy legislation, how it operates in practice, the constraints on its operation, etc. In my view it is not sufficient to mention that Tanzania has no comprehensive data privacy legislation. Perhaps an explanation for that would have been useful. It appears Ubena wants his audience to believe that once a comprehensive data privacy law is adopted in Tanzania, privacy will be automatically

erroneous belief that a comprehensive law will automatically guarantee the right to data privacy.[62] To avoid this shortcoming, this section extensively analyses the legal framework for data privacy protection in Nigeria. This is with a view to identifying some of the issues and challenges associated with it.

3.4.1. Constitutional protection of data privacy in Nigeria

The Constitution of the Federal Republic of Nigeria ('the Nigerian Constitution') is the *grundnorm* of the land and the *fons et origo* of Nigeria's jurisprudence.[63] It gives life to every other law in Nigeria.[64] The Constitution provides for the right to human dignity and one of the ways in which this right can be realised is through the protection of private and family life.[65] Section 37 expressly provides for the right to privacy. It specifies that '[t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.'[66] Section 45 of the Nigerian Constitution provides for the limitations to this right.[67] The Constitution does not, however, provide the meaning of privacy within the scheme of fundamental human rights. Nwauche gives some insights into the meaning of privacy as envisaged by the Constitution. He observes that there could be a general and specific understanding of privacy based on the constitutional provision:[68]

---

secured. This is certainly misleading because even in Europe privacy is infringed in the face of comprehensive data privacy legislation.' (n 59 above) 176.

62 Makulilo (n 59 above) 176.

63 JA Dada 'Human rights under the Nigerian Constitution: Issues and problems' (2012) 2(12) *International Journal of Humanities and Social Science* 43.

64 Indeed sec 1 of the Nigerian Constitution provides that it (the Constitution) is supreme and 'its provisions shall have binding force on the authorities and persons throughout the Federal Republic of Nigeria.' Sec 3 further provides that 'if any other law is inconsistent with the provisions of this Constitution, this Constitution shall prevail, and that other law shall, to the extent of the inconsistency, be void.' This implies that every other law must be in accordance with the Constitution for it to be valid.

65 Allotey AKE 'Data protection and transborder data flows: Implication for Nigeria's integration into the global network economy' unpublished LLD thesis, University of South-Africa, 2014 173.

66 Sec 37 of the Nigerian Constitution.

67 Sec 45 (1) provides that 'nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom of other persons.' The permissible derogation from the fundamental human rights provisions in the Constitution has also been criticised. It has been argued that they are 'too wide and in some cases, nebulous and antithetical to the cause of human rights.' Eg, the Constitution does not tell us the meaning of 'interest of defence', 'public safety', 'public order', 'public morality' and 'public health'. See Dada (n 63 above) 42.

68 ES Nwauche 'The right to privacy in Nigeria' (2007) 1(1) *Review of Nigerian Law and Practice* 84.

> Accordingly the use of the word 'the privacy of citizens' constitutes the general right in this section. Thus the use of the words '...their homes, correspondence, telephone conversations and telegraphic communications...' are the specific enumerations of the aforesaid general right.[69]

The author, however, observes that this understanding, even if accurate, does not help in our understanding of what is meant by a citizen's privacy.[70] This ambiguity may be a setback to the application of section 37 for the realisation of the right to data privacy protection in Nigeria. Nevertheless, Nwauche opines that deconstructing privacy can be done using his understanding from the premise of protection of privacy through the torts of breach of confidence and privacy.[71] He argues that, in either case, these torts as well as the constitutional right to privacy protect information.[72] Therefore, the constitutional provision on privacy in this context means it can be used for the protection of data privacy as:

> Informational privacy as a defining feature would then contextualise homes, correspondence, telephone conversations and telegraphic communications. On the other hand the nature of the interests that these specific words connote is predominantly that of information. Even though 'homes' could be ambiguous, 'correspondence, telephone conversations and telegraphic communications' clearly refer to information.[73]

In the same vein, Allotey argues that the reference by the Constitution to citizen's correspondence, their telephone and telegraphic communications envisages an intention to protect information privacy as information privacy involves protection of an individual against unlawful interference with his personal information held by other persons.[74] The scope of information privacy covers collection, storage, usage and dissemination of personal information by both public and private bodies.[75] The Constitution, therefore partially guarantees data privacy based on the scope of the right to privacy. As was earlier pointed out in the previous chapter, however, information privacy is only an aspect of the law on data privacy and as a consequence, it cannot be said that an individual's right to data privacy is effectively guaranteed by the constitutional provision.[76]

---

69 Nwauche (n 68 above) 84.
70 Nwauche (n 68 above) 84.
71 Nwauche (n 68 above) 84.
72 Nwauche (n 68 above) 84.
73 Nwauche (n 68 above) 84.
74 Allotey (n 65 above) 175.
75 Allotey (n 65 above) 175.
76 DW Schartum 'Designing and formulating data protection laws' (2008)18 *International Journal of Law and Information Technology* 2

The above opinions of Nwauche and Allotey have shown the possibility of extending the constitutional provision on the right to privacy to protect data privacy in Nigeria. An important question is what kind of activity should be carried out on personal data for it to be said that the constitutional provision has been violated? Will a mere accumulation of personal data be sufficient to constitute a violation of the right to privacy or must there also be use and/or disclosure? Nwauche argues that 'the Constitution concentrates on the information and therefore the acquaintance and public disclosure of the information is actionable.'[77] Thus, there is a violation of the right to information privacy as provided for in the Constitution if there is acquisition (collection) and/or disclosure of personal information. It must, however, be stated that the acquisition and/or disclosure must be in an unlawful manner, for there to be a breach of section 37 of the Nigerian Constitution. All these show the extremely narrow confines within which the Constitution operates in the protection of data privacy in Nigeria.

Another major criticism of section 37 on the protection of data privacy is that it applies to only Nigerians and therefore, it is discriminatory.[78] This is because the initial words of the section provide that 'the privacy of citizens…'[79] It can therefore be argued that a non-citizen cannot move the Nigerian courts to have his/her right to privacy enforced, let alone his/her right to data privacy. The African Charter on Human and Peoples' Rights (ACHPR), however, provides in article 7 that '[e]very individual shall have the right to have his cause heard.[80] This comprises: the right to an appeal to competent national organs against acts violating his fundamental rights as recognized and guaranteed by conventions, laws, regulations and customs in force.' It may therefore be argued that non-citizens could approach national institutions for the enforcement of their right to data privacy based on this provision.[81] The chance of success of such action is very remote as the Constitution is

77 Nwauche (n 68 above) 84.

78 See Kusamotu (n 18 above) 154. Dada also argues that the same discrimination exists with several other rights in the Nigerian Constitution for example the right to own immovable property in sec 43. He contends that such constitutional provisions are unreasonable and unjustifiable as 'there is nothing about the rights under consideration to justify or warrant limiting their enjoyment to Nigerian citizens only' Dada (n 63 above) 42.

79 Sec 37 of the Nigerian Constitution.

80 Art 2 of the ACHPR provides that every individual shall be entitled to enjoyment of rights recognised in the Charter. This provision is also limited as the Charter does not provide for the right to privacy let alone the right to data privacy. However, prohibition of discrimination in enjoyment of rights can be deduced from the same provision which states that such right guaranteed may be enjoyed 'without distinction of any kind such as race, ethnic group, colour, sex, language, religion, political or any other opinion, *national and social origin*, fortune, birth or other status.' (Emphasis added)

81 Art 7 of the ACHPR.

supreme[82] and any law inconsistent with the Constitution is null and void to the extent of its inconsistency.[83] In this case, article 7 of ACPHR is apparently inconsistent with the Constitution. Thus, personal data of non-Nigerians processed in Nigeria cannot be protected by section 37 of the Constitution.

That notwithstanding, the 'added value' of a right to data privacy will make section 37 extremely limited for both Nigerian and non-Nigerians. As was argued in the previous chapter,[84] the right to data privacy covers a wider scope in terms of protection of data privacy than the right to privacy. The *sui generis* right to data privacy is more properly placed to protect the autonomy and dignity of individuals in the information society by regulating the use of their personal data by both public and private data controllers.

A further issue with the application of section 37 of the Constitution for the protection of the rights to privacy and data privacy is the controversies on the possibility of enforcing fundamental rights by individuals against other individuals.[85] The prevalent view is that Nigeria's human rights jurisprudence only contemplates vertical application of human rights and not its horizontal application.[86] This opinion will no doubt have the effect of limiting the applicability of section 37 in protecting the right to data privacy. It will therefore be absurd to argue that section 37 cannot be applied against another individual. Hence, it is contended that 'the preponderance of judicial and academic opinion is that human rights can be enforced by individuals against other individuals'.[87]

It is important to state that the inclusion of the right to privacy in the Constitution has certain implications. First, the legislature may not pass any law or take any action which unreasonably restricts the right to privacy. Second, the provision on the right to privacy imposes an obligation on the legislature to enact a law to protect the privacy of personal data.[88]

---

82 Sec 1 of the Nigerian Constitution.
83 Sec 3 of the Nigerian Constitution.
84 Chapter 2 (2.6.3).
85 Nwauche (n 68 above) 88.
86 Nwauche (n 68 above) 88, vertical application of human rights means constitutional provisions on human rights can be enforced against the state and not individuals. Horizontal application means provisions on fundamental rights can be enforced against both the state and other individuals.
87 Nwauche (n 68 above) 88, moreover, Sec 1(1) of the Constitution provides that its provisions shall be applicable to all persons and authorities in the Federal Republic of Nigeria.
88 This was stated by Neethling with regard to the South African Constitutional provision on Privacy. See J Neethling *et al Neethling's law of personality* (2005) 271-273. See also A Roos 'Data protection' in D

3.4.2. Protection of data privacy in the African Charter on Human and Peoples' Rights (ACHPR)

The ACHPR,[89] arguably, also forms part of the legal framework for data privacy protection in Nigeria. This is because it is the primary human rights instrument in the Africa. Paradoxically, unlike other human rights instruments, it does not contain the right to privacy.[90] Authors try to seek justification for this manifest oversight. Olinger *et al* contend that the failure to mention privacy in the ACHPR 'indicates that privacy was simply not seen as a necessary right for Africans to live freely and peaceable.'[91] Based on this argument, realising freedom and peace on the African continent was taken to be part of the main objectives of the ACHPR and the human right to privacy was perceived as unnecessary for the actualisation of such objectives. Similarly, Allotey points out that

---

Van der Merwe *et al Information & communication technology law* (2008) 354. It is submitted that the constitutional provision has the same implication under the Nigerian Constitution. Moreover, sec 39 (3) of the Nigerian Constitution, in providing for the right to freedom of expression, stipulates that 'nothing in this section shall invalidate any law that is reasonably justifiable in a democratic society - (a) for the purpose of preventing the disclosure of information received in confidence…' Laosebikan therefore contends that 'this provision does not directly safeguard the protection of information or data, but it supports the enactment and enforcement of laws made for the purpose of protecting information received in confidence provided such laws are reasonably justifiable in a democratic society'. FO Laosebikan 'Privacy and technological development: A comparative analysis of South African and Nigerian Privacy and Data Protection Laws with particular reference to the protection of privacy and data in internet cafes and suggestions for appropriate Legislation in Nigeria' unpublished Ph.D. thesis University of Kwazulu-Natal, 2007 408.

89 The ACHPR also referred to as the 'Banjul Charter' is a primary regional human rights instrument in Africa. It was adopted in Nairobi Kenya on 27 June 1981 and came into force on the 21 October 1986.The ACHPR was domesticated in Nigeria via ACHPR (Ratification and Enforcement) Act of 1983 (formerly Cap 10 Laws of the Federation of Nigeria (LFN) 1990), now Cap A9 LFN 2004. It was domesticated in Nigeria pursuant to sec 12 of the Constitution. The legal effect of the Charter has been pronounced upon by the Supreme Court of Nigeria. It was held, per Ogundare JSC, that 'the African Charter is now part of the laws of Nigeria and like all other laws the Courts must uphold it'. The court went further to state that 'if there is a conflict between it and another statue, its provisions will prevail over those of that other statue for the reason that it is presumed that the legislature does not intend to breach an international obligation.' See *General Sani Abacha & 3 Ors v Chief Gani Fawehinmi* (2000) 4 SCNJ 401. Despite this clear pronouncement, there are still uncertainties regarding its status. For more on this, see AA Oba 'The African Charter on Human and Peoples' Rights and ouster clauses under the military regimes in Nigeria: Before and after September 11' (2004) 4(2) *African Human Rights Law Journal* 275-303.

90 A subsequent document, the African Charter on the Rights and Welfare of the Child (1990), however, mentioned privacy in a limited context. It provides in art. 10 that 'no child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.' A copy of the instrument is available in http://www.au.int/en/sites/default/files/Charter_En_African_Charter_on_the_Rights_and_Wlefare_of_the_Child_AddisAbaba_July1990.pdf (accessed 1 November 2015). Olinger *et al.* point out that 'it is somewhat strange that privacy is mentioned as a right for a child in the Charter of 1990 but has not been mentioned in the earlier Charter of 1981 as a right for all human beings.' HN Olinger *et al* 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa' (2007) 39 *The International Information & Library Review* 37.

91 Olinger (n 90 above) 37.

despite the Universal Declaration of Human Rights' (UDHR) and the International Convention on Civil and Political Rights' (ICCPR) influence on the Bills of Rights of many African countries, 'the political leadership of these countries… did not deem privacy as one of the human or peoples' rights that should be protected.'[92] The question therefore is that why will African leaders who played active role in the coming into force of the ACPHR consider privacy necessary for their individual countries but not important at the regional level?

What is clear from the above is that parties to the ACHPR do not consider the right to privacy as an important norm at the regional level. Thus, it was not thought necessary to expressly provide for privacy. Nevertheless, the right to privacy may be impliedly read into some of the provisions of the ACHPR. Articles 10 and 11, for example, provides for freedom of association and assembly.[93] London contends that 'the right to assemble freely with others also implies a right not to assemble' that is, to remain in solitude.[94] In the context of data privacy, freedom to assemble or associate will also include a right not to have one's personal information shared in an assembly or association. This is as far as the ACPHR goes in providing for privacy related interests of individuals.

That notwithstanding, the ACPHR provides for the right to receive and disseminate information. Article 9 provides that 'every individual shall have the right to receive information.' Certain questions arise from this provision. Does the provision also mean the right to access to information?[95] The provision also questions the kind of information that an individual is entitled to receive. Is it an individual's personal information in the hands of others (say government or private entities)? Or is it information about others or public information? If the section is interpreted to mean right to receive personal information, then it could be argued that the ACHPR also provides for the right of access to information

---

92 Allotey (n 65 above) 188.

93 Art 11 provides that 'every individual shall have the right to assemble freely with others. The exercise of this right shall be subject only to necessary restrictions provided for by law, in particular those enacted in the interest of national security, the safety, health, ethics and rights and freedoms of others.'

94 RW London 'Comparative data protection and security law: A critical evaluation of legal standards' unpublished LL.D thesis, University of South Africa, 2013 188.

95 Eg, art 3 of the ACHPR provides that 'the right of access to information' covers the right of the beneficiary to *seek and receive information* and the obligation of bodies of public authority to make access to the requested information possible, or to publicize information even when there is no special request for them, rather publication is their obligation according to individual laws or other general regulations.' (Emphasis added).

which is an important component of the law on data privacy. The position of this, however, remains unclear.[96]

Another argument that can be made on the justiciability of the ACHPR with regard to the protection of data privacy in Nigeria is based on article 7 which provides that:

> Every individual shall have the right to have his cause heard. This comprises: (a) the right to an appeal to competent national organs against acts violating his fundamental rights as recognized and guaranteed by conventions, laws, regulation and customs in force.

Based on the above provision, an individual can approach appropriate national institutions for the enforcement of his/her fundamental human right as guaranteed by any international agreement 'in force.' However, certain issues arise with regard to the applicability of this provision for the enforcement of data privacy right in Nigeria. The first issue is the meaning of the phrase 'in force' in the provision. Does it mean such international agreement which provides for the human rights must be ratified only or ratified and domesticated for it to be 'in force'? Also, since Nigeria is a state party of regional institutions with treaties on data privacy like the ECOWAS Supplementary Act,[97] can a person have his/her matter on infringement of data privacy heard by the courts? These uncertainties make article 7 of the ACHPR limited in protecting data privacy in Nigeria.

3.4.3. Common law protection of data privacy in Nigeria

The English common law may be applied for data privacy protection in Nigeria. Common law is an integral part of the received English law which is applicable in Nigeria.[98] The

---

96 Efforts to seek more clarification on the above provision yielded no results as an extensive search for the explanatory memorandum of the ACHPR proved abortive.

97 By virtue of the fact that it is directly applicable because it is an integral part of the ECOWAS Treaty. See 3.8.3 below for more discussion on the ECOWAS and data privacy in Nigeria.

98 The Common law is defined as the basic law of England which was developed by judges of the old common law courts out of the general customs and practices among the English communities in the early centuries. It is one of the received English laws applicable in Nigeria, others being doctrines of equity and Statute of General Application. The three English laws were received by the Interpretation Act Cap 89 Laws of the Federation and Lagos. See generally N Tobi *Sources of Nigerian law* (1996)17-58; AO Obilade *The Nigeria legal system* (1979) 69-82; AEW Park *The sources of Nigeria law* (1963) 5-14. G Ezejiofor 'Sources of Nigeria law' in CO Okonkwo (ed) *Introduction to Nigerian law* (1980) 1-54; AM Olong *The Nigerian legal system* 2nded (2007) 11-20; C Mwalimu *The Nigerian legal system* (2009) 27-29. The confluence of various laws under the Nigerian legal system makes a commentator describe law in Nigeria as a 'plural complex'. AA Oba '"Neither fish nor fowl": Area courts in the Ilorin emirate in Northern Nigeria' (2008) 58 *Journal of Legal Pluralism* 69.

English common law applies in Nigeria subject to the provisions of any other federal law[99] and 'so far… as the limits of the local jurisdiction and local circumstances shall permit'.[100] Since there is no other general federal law that specifically provides for data privacy protection, it is submitted that the common law applies to protection of data privacy in Nigeria. However, the English common law will not apply in areas of personal data processing that have been covered by other legislation.

The above, however, presents a simplistic view of the influence of common law in Nigerian jurisprudence. The attitude of the Nigerian courts towards the common law has always been an issue. The Nigerian courts seem to be at a loss as to the weight to be attached to the English common law. With regard to privacy generally, it can be argued that the English common law plays a significant role because of the relatively weak jurisprudence on the subject. The English common law may therefore be said to be binding. Nwauche shares a similar view. He opines that:

> In an environment where it cannot be said with any certainty that English common law is regarded as binding by Nigerian courts or is of persuasive authority given the manner in which Nigerian courts weave seamlessly in and out of English law, it is plausible to argue that the present English law on the subject could be regarded as binding by Nigerian courts.[101]

Historically, the English common law which is applicable in Nigeria does not recognise an independent tort of privacy.[102] This is unlike the approach adopted in civil law

---

99 The Interpretation Act (Cap 192, LFN 1990 now Cap I23 LFN (2004) provides in sec 32(1) that '[s]ubject to the provisions of this section and except in so far as other provision is made by any Federal law, the common law of England and the doctrines of equity, together with the statutes of general application that were in force in England on the 1st day of January, 1900, shall, in so far as they relate to any matter within the legislative competence of the Federal legislature, be in force in Nigeria.' An author, however, opines that 'it is generally acceptable by commentators that the cut-off date of January 1, 1900 applies only to English statutes and not the rules of common law and equity, and that the principles of common law and equity which are applicable in Nigeria are those which are current in England at any given time, so long as they are not inconsistent with any applicable Nigerian Statute or decision of a Nigerian court and subject (i) to the overriding power of the Nigerian Court to determine what is the current law of England and (ii) the duty placed upon the Nigerian courts by the statutes to apply English law only so far as the limits of local jurisdiction and local circumstances permit.' G Kodilinye *Nigerian law of torts* (1982) 10-11.

100 Interpretation Act (n 99 above), sec 32(2).

101 Nwauche (n 68 above) 67.

102 D Lindsay & S Ricketson 'Copyright, privacy and digital rights management' in AT Kenyon & M Richardson (eds) *New dimensions in privacy law: International and comparative perspectives* (2006) 121. For more detailed analysis on the relationship between the common law privacy and breach of confidence, see R Wacks 'Why there will never be an English common law privacy tort' in Kenyon & Richardson (eds) *New dimensions in privacy law: International and comparative perspectives* (2006) 154.

jurisdictions.[103] The courts in common law jurisdictions rely on the equitable action of breach of confidence to protect privacy.[104] Thus, by an extended action for breach of confidence, the common law protects private information.[105] Recently, though, the invasion of privacy is now being recognised as an independent tort under the common law in England.[106] However, the Nigerian jurisprudence based on the common law is not that advanced to recognise an independent tort of privacy.

An action for breach of confidence as a means of protecting data privacy seems to be inadequate. Breach of confidence involves a violation of trust within a particular relationship,[107] which means there must be a relationship between the parties.[108] However, many data privacy breaches occur in circumstances where there is no form of relationship between the parties.[109] This is so especially for violation of data privacy by public data controllers.

It follows from the above that the major means by which data privacy can be protected in Nigeria through the common law is by the equitable action of breach of confidence. That

---

103 Like Germany and South Africa where there is an independent protection of privacy under the civil law of delict. These two countries do not have torts laws rather privacy is recognised and protected as a personality right under the law of delict.

104 *Vidal-Hall & Ors v Google Inc* (2014) EWHC 13 (QB).

105 Indeed in the *Vidal's* case, the court observed that it may be correct to state that the tort of invasion of privacy is unknown in English law however, it will be wrong to say that the specific tort of misuse of private information is unknown in English law. (See para 66). Where a person discloses his personal information to another person in which a duty of confidence is imposed, if that other person discloses such information, then an action could lie for breach of confidence. Eg duty of confidentiality between patients and doctors. See Laosebikan (n 88 above) 340.

106 See *Imerman v Tchenguiz* (2011) Fam 116, para 65.Thus in *Campbell v MGN* (2004) UKHL 22, the right to privacy was recognised by the House of Lords 'in the form of protection against the publication of private facts that fell within the expanded parameters of the action for breach of confidence'. See Lindsay & Ricketson (n 102 above) 137. The authors further state that 'one way to interpret this development is as a creative, but potentially fraught, fusion of a 'rights-based' conception of privacy, reflecting the influence of European Convention on Human Rights, with the traditional incremental approach of the English common law.'

107 DJ Solove '"I've got nothing to hide" and other misunderstandings of privacy' (2007) 44 *San Diego Law Review* 770.

108 This is also manifest from the requirements of an action for breach of confidence. The requirements for a tort of breach of confidence were outlined in *Coco v AN Clark (Engineers) Ltd* (1969) RPC 41, 47. They are: '(1) the information must have the necessary quality of confidence about it; (2) *the information must have been imparted in circumstances importing an obligation of confidence*; and (3) there must be an unauthorised use or disclosure of that information to the detriment of the party communicating it.' A commentator has, however, opined that 'the law has gone further to infer an obligation of confidentiality even when the parties do not know each other if by conduct there is notice that some confidentiality exists.' (Emphasis added) Nwauche (n 61 above) 75.

109 In the UK, the criteria of 'prior relationship' for an action for confidentiality to stand seems to have been relaxed a little. Thus, in *WB v H Bauer Publishing Ltd* (2002) EMLR, it was held that for an action for obligation of confidence can arise in equity without any prior existing relationship between the parties. See G Phillipson 'Transforming breach of confidence? Towards a common law right of privacy under the Human Rights Act' (2003) 66 *Modern Law Review* 726.

notwithstanding, some principles of data privacy can be seen in the common law, especially where misuse of personal information amounts to a tort. [110] For example, the torts of trespass,[111] defamation,[112] nuisance,[113] passing-off [114] and intentional infliction of emotional distress could be resorted to for common law protection of personal information.[115]

The common law protects intrusion into a person's private space and prevents the disclosure of certain private information. This means it gives an individual the right to determine the destiny of his personal information. It also helps protect his identity. These are very important aspects of the right to data privacy protection. However, the common law jurisprudence on data privacy protection and privacy has generally been too limited to adequately protect individuals' personal data as it does not incorporate the basic principles of data privacy.[116] Moreover, what the common law actually protects is private information which may not necessarily be personal data.[117]

3.4.4. Analysis of the constitutional and common law protection of data privacy

The essence of data privacy law is to give individuals control of their personal information as it is an embodiment of their personality. Impliedly, this means an individual should be able to determine what happens to his/her personal information. Putting individuals in control of their personal information can be done in two ways: by guaranteeing both the

110 Laosebikan (n 88 above) 340.

111 Eg, where information is obtained by means of unlawful entry into a person's land or property, an action may lie in the tort of trespass. Particularly, where a person takes storage devices containing personal information of another person, accesses and uses the information, an action could lie for trespass to property. Laosebikan (n 88 above) 341-342.

112 Where the disclosure or publication of personal information causes injury to the reputation of a person, an action for the tort of defamation could lie. Laosebikan (n 88 above) 343-344.

113 Eg, where personal data is obtained by interference into ones peaceful enjoyment of his/her property, that amounts to nuisance. Eg, where personal information is obtained from a surveillance camera installed. Laosebikan (n 88 above) 343.

114 Where the misuse of business information involves imitation of the plaintiff's name or business idea in such a way that the public is misled into thinking the business is same with the plaintiff's, liability for passing off shall lie in respect of unlawful use of personal information. Laosebikan (n 88 above) 344.

115 Laosebikan (n 88 above) 344.

116 It is not as developed as the common law of other jurisdictions like South Africa, which recognises an independent personality right of privacy and identity under the law of delict. A Roos 'The law of data (privacy) protection: A comparative and theoretical study' unpublished LL.D thesis, University of South Africa, (2003) 545; See also J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of delict' (2012) 75 *Tydskrif vir hedendaagse Romeins-Hollandse Reg (THRHR)* 234.

117 Eg, one's name and phone number may not be secret or confidential but it is personal information within the scope of data privacy law so far as it capable of identifying a person. See Abdulrauf (n 49 above) 74.

opacity and transparency of their personal data as the case may be.[118] In other words, data privacy mainly operates based on two broad notions - the permissive[119] and prohibitive notions.[120] Data privacy law does not make personal information inaccessible or private (secret or confidential) outright. The value attached to personal data and its uses will make this impracticable. A data privacy law must make personal data accessible (to both individuals and legitimate data controllers) or permit its processing - provided certain rules are followed.[121] Data privacy law, therefore does not proscribe the use of individuals' personal data, but facilitates its use in a rights respecting manner.[122] Based on the idea that data privacy does not completely prohibit the processing of personal data, there is therefore the need to grant individuals certain powers in the form of rights over their personal information. This is so as to facilitate their access to ensure that the data is accurate, complete and up to date. Data privacy laws incorporate several principles which enable individuals to exercise these rights. The principles include: the principles of fairness, accountability, openness, data subject participation.[123] In fact, De Hert and

---

118 Transparency is a tool used to hold data controllers accountable for personal data in their possession. Opacity on the other hand refers to inaccessibility of personal data i.e. restriction in the processing of personal data. Some authors point out that 'data protection laws were precisely enacted not to prohibit, but to channel power, viz; to promote meaningful public accountability, and provide data subjects with an opportunity to contest inaccurate or abusive record holding practices.' P De Hert & S Gutwirth 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes *et al Privacy and the criminal law* (2006) 78.

119 'Permissive notion' in this context means two things. First, in relation to data controllers, it allows them to process personal data subject to certain explicit procedural rules. Second, with regard to data subjects, the permissive notion enable them access to their personal data in the hands of a data controllers.

120 Regarding the right to personal data protection in Europe, some authors point out that 'it oscillate between two poles. A first approach envisages the right as representing, in substance, an overall prohibition of the processing of personal data – thus, as what could be labelled a *prohibitive* notion. A second approach conceives of the right as constituting instead, in essence, a series of rules applying to the processing of personal data, regulating and limiting such processing but not forbidding it- or as a *permissive* (or regulatory) notion.' GG Fuster & S Gutwirth 'Opening up personal data protection: A conceptual controversy' 29 *Computer Law & Security Review* (2013) 531-539.

121 It has been pointed out that data (privacy) protection 'is pragmatic in nature: it assumes that private and public actors need to be able to use personal information and that this in many cases must be accepted for societal reasons. The 'thou shall not kill' that we know from criminal law, is replaced by a totally different message: 'thou can process personal data under certain circumstances'. See De Hert & Gutwirth (n 118 above).

122 Indeed it has been observed that 'the main aims of data protection consist in providing various specific procedural safeguards to protect individuals' privacy and in promoting accountability by government and private record-holders.' De Hert & Gutwirth (n 118 above) 77.

123 It was pointed out that '…data protection regulations create a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal. As such these regulations implicitly accept that a processing of personal data is closely linked to the exercise of power and that it facilitates its establishment.' De Hert & Gutwirth (n 118 above) 78.

Gutwirth argue that the law on data privacy is to act mainly as a tool of transparency - obviously ignoring the opacity function of data privacy.[124]

The forgoing analysis of the constitutional and common law protection of data privacy (in the previous section) shows that they operate based on only one notion of data privacy law - they merely prohibit the use of private information; that is, the prohibitive notion. Without a doubt, prohibiting the use of individuals' personal data in certain circumstances is one of the objectives of data privacy, but that is not the sole objective. An outright prohibition on the use of personal data will cause hardship to individuals in this information society. It will negatively affect e-commerce and the society in general. As a consequence, the constitutional and common law protection of data privacy in Nigeria show considerable flaws relating to the overall objective of data privacy law. Neither the Constitution nor the common law has provisions which enable an individual to have access to his/her personal information in the hands of others (private or public entities). This is a tool of transparency which the rules of data privacy protection seek to enhance. It is also an instrument of power granted to individuals to ensure they are in control of their personal information.

The constitutional and common law provisions on data privacy show that the information which is being protected is private information which has the element of secrecy or confidentiality. The scope of the regime of data privacy protection covers personal data/information which does not necessarily have to be secret or confidential information.[125] It suffices if such data merely identifies an individual. This means information, such as an individual's phone number or address, which is not necessarily private, is personal data under data privacy law and accumulation of this category of information poses significant threats to such an individual.

3.5. Legislative protection of data privacy in Nigeria (sectoral and other laws)

Apart from the above stated laws that partially regulate the processing of personal data, other laws also have provisions which protect data privacy. These laws are, however, of

---

124 De Hert & Gutwirth (n 118 above) 78. In the words of the authors, '[d]ata protection regulations mainly belong to the tools of transparency, as opposed to the protection of privacy that pertains to the tools of opacity.'

125 Abdulrauf (n 49 above) 74.

very limited application as they apply only to particular sectors or specific activities of data processing. Some of these statutes include: the Evidence Act,[126] the Nigeria Postal Service (NIPOST) Act,[127] Wireless Telegraphy Act[128] and the Telecommunications and Postal Offences Act.[129] This section will not consider the provisions of these laws in detail for two reasons. Firstly, they are of extremely limited application and secondly, most of the provisions of these laws do not envisage the current issues of data privacy in the digital society analysed in part 3.3 above. For example, the Wireless Telegraphy Act still has provisions on antiquated methods of information transfer via telegraph post. The use of the internet and new technologies has far outgrown that and presents new dimensions to data privacy challenges. In the light of the forgoing, this section considers only sectoral laws of contemporary significance to data privacy protection.

3.5.1. Freedom of Information Act (FOIA) 2011

In a bid to ensure greater transparency and accountability in governance,[130] the Nigerian government enacted the Freedom of Information Act 2011 (FOIA).[131] The FOIA makes public records and information available and provides public access to records and information.[132] The Act protects public records in a way consistent with public interest and protection of personal privacy.[133] In relation to data privacy protection, the FOIA provides that a public institution must deny an application for information that contains personal

126 The Nigerian Evidence Act 2011. Formerly Cap E 14 LFN 2004, sec 161 (3).
127 Nigeria Postal Service Act Cap N127 LFN 2004, secs 28 & 29.
128 Wireless Telegraphy Act (1961) now no 31 (1998), sec 10.
129 Telecommunications and Postal Offences Decree 1995 (formally Decree No 13 of 1995 now Advance Fee Fraud and Other Related Offences Act 1995), secs 18 & 25.
130 See GK Nwamu 'A critical analysis of Freedom of Information Act, 2011' in E Azinge & F Waziri (eds) *Freedom of information law & regulation in Nigeria* (2012) 1. See also O Eruaga 'The first year of the freedom of information Act: Has it been tested?' E Azinge & F Waziri (eds) *Freedom of information law & regulation in Nigeria* (2012) 22.
131 The FOIA is an enactment of the Nigerian National Assembly assented to by the President on the 28th of May 2011 available at http://www.nigeria-law.org/Legislation/LFN/2011/Freedom%20Of%20Information%20Act.pdf (accessed 1 November 2015).
132 The long title to the FOIA states that it is '[a]n Act to make public records and information more freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy, protect serving public officers from adverse consequences of disclosing certain kinds of official information without authorization and establish procedures for the achievement of those purposes and; for related matters.'
133 FOIA, long title.

information.[134] The provision further gives examples of such personal information which should not be accessible to the general public. They include:

> (a) files and personal information maintained with respect to clients, patients, residents, students, or other individuals receiving social, medical, educational, vocation, financial, supervisory or custodial care or services directly or indirectly from public institutions; (b) personnel files and personal information maintained with respect to employees, appointees or elected officials of any public institution or applicants for such positions; (c) files and personal information maintained with respect to any applicant, registrant or licensee by any government or public institution cooperating with or engaged in professional or occupational registration, licensure or discipline; (d) information required of any tax payer in connection with the assessment or collection of any tax unless disclosure is otherwise requested by the statute; and (e) information revealing the identity of persons who file complaints with or provide information to administrative, investigative, law enforcement or penal agencies on the commission of any crime.[135]

The FOIA is supposed to promote one of the main objectives of the right to data privacy protection which is enhancing access to information in order to reduce the power asymmetries or imbalance in power between the individuals and the state.[136] What this implies is that an individual should be given access to public records containing his/her personal information. However, it is not clear whether an individual will be able to gain access to his/her personal information in the hands of public bodies via the FOIA. One may argue that such is possible as there is nothing in section 14 which suggests otherwise. The categories of personal information which should be denied access, as highlighted in the above section, do not include personal information of the requester although, the section uses the word 'includes' which means the list is not exhaustive. The position of an individual having access to his/her personal information under the FOIA therefore remains uncertain.

An individual may, however, rely on section 14 (2) to gain access to his personal information as the section provides that 'a public institution shall disclose any information that contains personal information if - (a) the individual to whom it relates consents to the disclosure'.[137] Thus, the situation will be as good as arguing that an individual consents to disclosure of his/her personal information. Moreover, based on section 1(2) of the Act, 'an

134 FOIA, sec 14 (1).
135 FOIA, sec 14(1)
136 O Lynskey 'Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order' (2014) 63(2) *International and Comparative Law Quarterly* 593.
137 FOIA, sec 14 (2).

applicant need not demonstrate any specific interest in the information being applied for.'[138]

The limitation of the FOIA with respect to data privacy protection is that it is only applicable to publicly held records.[139] An individual does not have access to records held by private entities (such as private data controllers) by virtue of the law. Another limitation is that the FOIA only provides for access to public records, but does not suggest that such records could be corrected or updated based on the principles of data processing. Furthermore, the definition of personal information in the FOIA shows that it is limited to 'official information held about an identifiable person.'[140] This is far narrower than 'any information which reasonably identifies a data subject' based on the general principles of data privacy law.[141] In any case, as the name suggests, the law is merely an access to information law and nothing more.

3.5.2. The National Health Act 2014

The much anticipated National Health Act[142] that is expected to revolutionise the health sector was recently passed into law.[143] It contains some provisions which could be argued to be in accordance with the general objectives of a data privacy law. Part III of the Act contains rights and duties of users and health care personnel. The Act provides for an obligation to keep health records of every user of the health service on the person in charge of every health establishment.[144] It also provides that all information concerning a user

138 This provision has, however, been severely criticised as being vague. See Nwamu (n 121 above) 5-7.
139 FOIA, sec 1 & long title.
140 FOIA, sec 30 (3).
141 Art 2 of the EU Directive. There are many other criticisms of the FOIA which is outside the scope of this work. Nwamu, for example, points out that 'it has been observed that the FOIA contains more exemption sections that the sections that grant access to information to Applicants. It can be seen that only Sections 1 and 3 grant access to information, while ten sections (sections 7, 11, 12, 14, 15, 16, 17, 18, 19 and 26) are designed to disallow or deny the public access to information.' Nwamu (n 130 above) 18-19.
142 Available at http://www.unicef.org/nigeria/ng_publications_national_health_bill_2008.pdf (accessed 1 November 2015).
143 On 19 February 2014, the Nigerian Senate passed the National Health Bill 2014, which is to 'revolutionise' the health sector and focus heavily on better regulation and quality. The Bill is for an Act to provide '[a] Framework for the Regulation, Development and Management of a National Health System and set Standards for Rendering Health Services in the Federation, and Other Matters Connected therewith', http://www.hanshep.org/news-and-events/nigeria-passes-national-health-bill-2014 (accessed 1 November 2015). The Bill was signed into law by the former Nigerian President on 9 December 2014. See A Chiejina 'Jonathan finally signs National Health Bill into law' *Business day* http://businessdayonline.com/2014/12/president-jonathan-finally-signs-national-health-bill/#.VKkvuNLF9yI (accessed 1 November 2015).
144 National Health Act, sec. 25.

relating to his/her health status, treatment or stay in a health establishment is confidential[145] and no person may disclose any information contemplated in the subsection except under certain circumstances which include consent,[146] order of court[147] and if non-disclosure represents a serious threat to public health.[148] The Act also obliges a person in charge of a health establishment who is in possession of a user's health record to set up control measures to prevent unauthorised access to those records and the storage facility in which or the system by which they are kept.[149] Finally, the Health Act provides for liability for failure to comply with this provision.[150]

Even though the Act requires health practitioners to keep extensive health records of users of health services, it only imposes a duty of confidentiality on health providers.[151] It does not provide a special regime for protection of personal data contained in health records. The only principle of personal data protection that appears to have been sufficiently provided for in the Act is the safeguard principle.[152]

3.5.3. Statistics Act 2007

The Statistics Act[153] establishes the National statistical system which comprises of producers of statistics, data users, data suppliers, and research and training institutions.[154] The objectives of the system among others include collection, processing, analysis and dissemination of statistical data.[155] The Act does not define statistical data, but it is submitted that it includes personal information. With respect to protection of personal data, section 26(1) provides that 'the provisions of this Act shall not affect any law relating to

145 National Health Act, sec. 26(1).
146 National Health Act, sec. 26 (2)(a).
147 National Health Act, sec. 26 (2)(b).
148 National Health Act, sec. 26 (2)(c).
149 National Health Act, sec. 29.
150 National Health Act, sec. 29 (2)(i) & (ii).
151 One may argue that such confidentiality of records is also covered under the common law tort of breach of confidence. However, the common law will be limited in this regard because it only applies where a data subject has given a health practitioner his/her information directly. The common law does not cover cases where personal information is gotten from other sources (especially lawful sources).
152 The person in charge of a health establishment, who is in possession of a user's health records, shall set up control measures to prevent unauthorised access to those records and to the storage facility in which, or system by which, records are kept.
153 A copy of the Act is available at http://www.nassnig.org/nass/includes/tng/pub/tNG_download4.php?pageNum_bill=4&totalRows_bill=193&KT_download1=8bc66b39f7076b83664721f21bd48ac4 (accessed 1 November 2015).
154 Statistic Act, sec 1(1) & (2).
155 Statistic Act, sec 2.

the disclosure or non-disclosure of any official, secret or confidential information or trade secret.' Subsection 2 is more apt on data privacy protection. It provides that:

> Data collected for statistical purposes shall be treated as confidential and data confidentiality means that the dissemination of these data (and the statistics which can be calculated from them) shall not permit the identification directly or indirectly of the units concerned and that a prohibition is imposed on data producers against disclosing information of an individual obtained in the course of their work.

3.5.4. Cybercrime (Prevention, Prohibition etc) Act 2015

Although cybercrime laws are not *suo moto* data privacy protection instruments, certain provisions may be interpreted as protecting personal information. The Cybercrime Act[156] is the most recent legislative instrument on cybercrime in Nigeria. Its primary objective includes to 'promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property *and privacy rights.*'[157] In section 38 of the Act, several duties of service providers are stipulated. One such duty is that:

> Anyone exercising any function under this section shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement.[158]

From the above provision, it is submitted that the Act protects privacy generally and not personal information *stricto sensu.* Nevertheless, the law identifies identity theft as a cybercrime punishable under the Act.[159] Identity theft is inturn defined as 'the stealing of somebody else personal information to obtain goods and services through electronic based transactions.'[160] Personal information is, however, not defined in the Act.

3.5.5. Analysis of the sectoral regime on data privacy protection

The significance of other legislation in the realisation of adequate data privacy protection cannot be overemphasised. This is a reason why many countries have other laws that make

156 Available at https://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention,etc)_Act,_2015.pdf (accessed 24 January 2016).
157 (Emphasis added). See Cybercrime Act, sec 1(c).
158 Cybercrime Act, sec 38(5).
159 Cybercrime Act, sec 22(1).
160 Cybercrime Act, sec 58.

extensive provisions for data privacy protection in addition to their omnibus data privacy laws. Schartum observes that:

> …a limited number of important data protection issues arise within the framework of legislation that first and foremost regulates other questions than those that could be regarded as relating to data protection. For data protection to be an influential force, it is important that selected elements are included as an integral part of other legislation.[161]

Moreover, the EU Directive requires, *inter alia*, that 'rules of law, both general and sectoral' be considered in determining adequacy of a data protection regime.[162] This shows the importance of other laws in data privacy protection.

A review of the laws of the major sectors that carry out personal data processing in Nigeria reveals two obvious facts. First, many of these sectors do not have a law in force which provide for protection of data privacy. Furthermore, the main legislation regulating these personal data processing activities do not provide for specific rules on the collection and use of individual's personal data. For example, the Nigerian Communications Act, which is the main law regulating the telecommunications sector, does not have any provision on data privacy.[163] A similar situation is also found in the banking sector.[164] In some cases, many of the sectoral laws are outdated. For example the Consumer Credit[165] and Consumer Protection Laws[166] in Nigeria have been in force since colonial and military era. This, therefore, depicts the unlikelihood of such laws having provisions on data privacy protection which is a relatively recent issue.

Similarly, relatively recent laws in sectors that process personal data do not provide for coherent provision on data privacy protection.[167] For example, the National Health Act was enacted in 2014.[168] One would have expected that because of the significant attention data privacy currently attracts, the Nigerian legislature would seize the opportunity to

161 Schartum (n 76 above) 17.
162 EU Directive, art 25(2).
163 The NCC will be analysed in detail in the next section of the chapter.
164 The CBN is the regulatory body for the banking and financial sector in Nigeria. Its primary legislation does not contain any provision on neither privacy nor data protection. See the CBN Act, No 7 2007.
165 The main law on consumer credit in Nigeria is the Money Lenders Ordinance 1927 which later became Money Lenders Act Cap 124 LFN 1958. These laws have, however, been repealed and what is now in existence is Money Lenders Laws of the states.
166 Consumer Protection Council Act C25 LFN 2004. It was formerly Decree No 66 of 1992 and has not been substantially revised since then.
167 By coherent provisions, I mean provision that set out the generally known principles of data processing and having a special provision for the protection of sensitive personal data.
168 The National Health Act was elaborately discussed in 3.5.2 above.

establish rules on data privacy in the Act. Such piece of legislation is expected to anticipate present and future challenges brought about by advances in ICT and make sufficient provisions for them. This is more so for the health sector that is known to have a vast amount of sensitive data in its possession. However, the Nigerian legislature did not have that foresight.

The forgoing analysis shows that Nigeria has no sectoral legislation that has coherent provisions on data privacy protection in line with international practices.

3.6. Institutions relevant to data privacy protection in Nigeria: Issues and challenges

3.6.1. Nigerian Communications Commission (NCC)

The communications sector in Nigeria possesses and controls a large amount of personal data. The NCC is the principal regulatory body of the communication sector. It is an independent national regulatory authority for the telecommunications industry.[169] The NCC's functions, among others, include the 'implementation of the Government's general policies on communications industry and the execution of all such other functions and responsibilities as are given to the Commission under this Act or are incidental or related thereto.'[170] The NCC also has the 'general responsibility for economic and technical regulation of the communications industry.'[171] The NCC is established by the Nigerian Communications Act 2003 (NCA).[172] Rather surprisingly, the NCA does not contain any provision on data privacy protection. This is disturbing because of the vast amount of personal data being processed in the telecommunications sector in Nigeria.

The compulsory SIM card registration scheme[173] is one issue which questions the regulatory function of the NCC especially as regard data privacy protection of telecom subscribers.[174] The NCC, pursuant to its mandate under sections 1(i) and 70 of the NCA[175]

---

169 See Nigeria Communications Commission http://www.ncc.gov.ng/ (accessed 1 November 2015).

170 Nigeria Communications Act (NCA) No 62 Vol. 90 (2003), Sec 4(1)(t). A copy of the NCA is available at http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=56&Itemid=65 (accessed 1 November 2015).

171 NCA, sec 4 (1)(w).

172 NCA, sec 3(1) provides that '[t]here is established a Commission to be known as the Nigerian Communications Commission with responsibility for the regulation of the communications sector in Nigeria.'

173 Discussed in section 3.3.1.1 above.

174 Pursuant to the NCC's directive published in *Thisday Newspaper* 31 December 2009.

made the SIM Card Registration Regulations of 2010.[176] The objective of the Regulation 'is to provide a regulatory framework for the registration of all SIM Card users, and for the control, administration, and management of the Central Database.'[177] The Regulation authorises the NCC to establish 'a central database of all recorded subscriber information to be known as the Central Database.'[178] A central database will definitely raise issues of data privacy protection. Section 10 of the Regulation provides that

> (1) Licensees shall take all reasonable precautions to preserve the integrity and prevent any corruption, loss or unauthorized disclosure of Subscriber Information retained pursuant to paragraph 9(5) and shall take steps to restrict unauthorized use of the Subscriber Information by its employees who may be involved in capture and or processing of such Subscriber Information.
> (2) The Subscriber Information shall not be transferred outside the Federal Republic of Nigeria.

The above section is the extent that the Regulation goes in providing for the protection of personal information.[179] The provision, not stipulating the FIPs, is manifestly inadequate in the protection of the personal information in the digital society.

Subsequently, the NCC made the Registration of Telephone Subscribers Regulation (RTS Regulation) 2011.[180] This Regulation has made more efforts towards protecting individuals' personal data collected by telecommunication companies and independent registration agents in view of their mandate to collate and retain data of subscribers under the Regulation. Section 9 titled 'data protection and confidentiality' provides that:

---

175 Sec 70(1)(g) of the NCA gives the NCC powers to 'make and publish regulations' for a range of issues including but not limited to matters as are necessary for giving full effect to the provisions of the Act and for their due administration.

176 See NCC Draft Regulation for the Registration of All Users of Subscriber Identity Module (SIM) Cards in Nigeria available at http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=72&Itemid= (accessed 1 November 2015).

177 NCC Draft Regulation for the Registration of All Users of Subscriber Identity Module (SIM) Cards in Nigeria, sec 2.

178 NCC Draft Regulation for the Registration of All Users of Subscriber Identity Module (SIM) Cards in Nigeria, sec 4.

179 The Regulation defines personal information in sec 1 as 'the full names (including father's first name), gender, date of birth, residential address, nationality, state of origin, occupation and such other personal information and contact details of Subscribers as the Commission may from time to time specify in a data dictionary for registration of SIM Card users.' NCC Draft Regulation for the Registration of All Users of Subscriber Identity Module (SIM) Cards in Nigeria, sec 1.

180 NCC (Registration of Telephone Subscribers) Regulation, vol 98, No 101 2011. A copy of the regulation is available at http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=74&Itemid=89 (accessed on 1 November 2015).

> 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.[181]

Unlike other data privacy provisions under the Nigerian legal framework, the RTS provides for the right of access, update and rectification of personal information[182] stored in the central database by a subscriber. This is a transparency tool and a fundamental objective of data privacy law. With regard to the 'opacity' objective of data privacy, section 9(2) provides for the confidentiality or secrecy of personal information. It provides that:

> The subscriber information contained in the Central Database shall be held on a strictly confidential basis and no person or entity shall be allowed access to any subscriber information on the Central Database except as provided in these Regulations.

The RTS Regulation further provides for the processing limitation principle in that subscribers' information is not to be used for any purpose other than what is required in the Regulations or in an Act of the National Assembly.[183] Section 9(4) also imposes the responsibility of safeguard of subscribers' personal information on licensees, Independent Registration Agents, Subscriber Registration Solution Providers and the NCC. The section provides that all precautions in accordance with international best practice must be taken to preserve the integrity of subscribers' personal information.[184] Finally, subscribers' personal information is not to be retained after transmission to the central database.[185]

The RTS does not exhaustively provide for the FIPs. The processing limitation, purpose specification and security safeguard principles appear to be the only principles that are provided for. Another limitation of the Regulation is with respect to the provisions on penalties. The Regulation provides that '[d]ealing with subscriber information inconsistent

---

181 NCC (Registration of Telephone Subscribers) Regulation, sec 9(1).
182 Personal information is defined by the regulation as including 'the full names (including mother's maiden name), gender, date of birth, residential address, nationality, state of origin, occupation and such other personal information and contact details of subscribers specified in the Registration Specifications. Sec 1(2).
183 NCC (Registration of Telephone Subscribers) Regulation, secs 9(3) & 9(5).
184 NCC (Registration of Telephone Subscribers) Regulation, sec 9(4)
185 NCC (Registration of Telephone Subscribers) Regulation, sec 9(6)

with the provisions of the regulations' attracts only a penalty.[186] It does not treat such as misuse of personal information that entitles the subscriber to compensation. Moreover, it is submitted that the fine imposed is a paltry sum compared to the huge profits made by telecom operators in Nigeria. The light penalty may be because the RTS is merely a Regulation with little or no binding force. That could also be a reason why there is no, to the best of this researcher's knowledge, any reported case of misuse of personal data pursuant to the Regulation.

3.6.2. National Information Technology Development Agency (NITDA)

The NITDA was established to create a framework for the planning, research, development, standardisation, application, coordination, monitoring, evaluation and regulation of IT practices, activities and systems in Nigeria.[187] Its main function is to develop IT in Nigeria through regulatory standards, guidelines and policies. [188] It is the primary institution responsible for e-government implementation, internet governance and general information technology (IT) development in Nigeria.[189] With regard to issues of IT, the NITDA is the foremost agency in Nigeria. An institution with broad mandates relating to IT is expected to push for policies on data privacy protection which is a prevailing IT issue worldwide. This is the reason why the Nigerian National Policy for Information Technology[190] (which the NITDA seeks to implement)[191] provides that Nigeria 'shall promote and guarantee freedom and rights to information and its use, protect individual privacy and secure justice for all by passing relevant Bills and Acts.'[192] One of the strategies in realising this goal is to 'ensure the protection of individual and collective

---

186 NCC (Registration of Telephone Subscribers) Regulation, sec 21. 'Any entity including licensees, independent registration agents or subscriber registration solution providers who retains, duplicates or deals with Subscriber's information in contravention of any of the provisions of these Regulations is liable to a penalty of N200,000.00 per Subscription Medium. (2) Where an entity, including licensees, independent registration agents or subscriber registration solution providers is found to have utilised a subscriber's information in any business, commercial or other transactions, such entity is liable to a penalty of N1,000,000.00 per Subscription Medium.'

187 National Information Technology Development Agency (NITDA) Act 2007. Sec 6(a). Also available at http://www.nitda.gov.ng/documents/NITDA%20act%202007.pdf (accessed 1 November 2015).

188 NITDA Act, sec 6. See also NITDA 'About us' http://www.nitda.gov.ng/about.html (accessed 1 November 2015).

189 NITDA (n 188 above).

190 Nigerian National Policy for Information Technology available at http://www.researchictafrica.net/countries/nigeria/Nigerian_National_Policy_for_Information_Technology_2000.pdf (accessed 1 November 2015). See general objective general objective xxxiii.

191 Allotey (n 65 above) 127.

192 Nigerian National Policy for Information Technology (n 190 above) 32.

privacy, security, and confidentiality of information.'[193] Nevertheless, no concrete data privacy legislation has been made pursuant to the general objectives of the NITDA. However, the NITDA issued the Guidelines on Data Protection[194] which is in line with the EU Directive.[195]

To ensure effective enforcement, it is provided that 'a breach of the Guidelines shall be deemed to be a breach of the Act.'[196] It is further provided that the 'Guidelines are mandatory for federal, state and local government agencies and institutions as well as other organisations which own, use or deploy information systems within Federal Republic of Nigeria.'[197] Nevertheless, it must be noted that Guidelines are not as effective as Acts of the National Assembly in protecting individuals' rights. This is because Guidelines do not have the necessary legal force as legislation do. Furthermore, the level of awareness of the existence of these Guidelines and the rights established therein appear to be significantly low.[198]

3.6.3. National Identity Management Commission (NIMC)

The National Identity Management Commission Act ('NIMC Act')[199] establishes the NIMC for the creation and 'maintenance of the national database, registration of

193 Nigerian National Policy for Information Technology (n 190 above) 33.

194 The Guidelines were issued pursuant to secs 6, 17 and 18 of the NITDA Act 2007. NITDA Guidelines on Data Protection (2013) available at http://www.nitda.gov.ng/documents/Guidelines%20on%20Data%20Protection%20Final%20Draft3.5%20Final.pdf (accessed 1 November2015).

195 The Guidelines applies to both public and private sector (sec 1.4). Sec 1.3 contains the scope of the Guidelines which covers data controller or processor or data subject operating within Nigeria and organisations based outside Nigeria if they process Nigeria citizens personal data. The Guidelines cover 'processing of personal data wholly or partly by automatic means and processing otherwise than by automatic means.' It is provided that the Guidelines do not cover the processing of personal data relating to public safety and national security. Sec 2.1 makes rules on data collection and processing generally. Sec 2.2 provides for the right of personal data access by their parties and data subjects. The Guidelines provide that organisations should 'designate an employee' as the organisation's Data Security Officer. His duties are listed in the Guidelines.The Guidelines also provide for 8 FIPs in sec 4. They are 1. Personal data must be processed fairly and lawfully; 2. Personal data shall only be used in accordance with the purposes for which it was collected; 3. Personal data must be adequate, relevant and not excessive; 4. Personal data must be accurate and where necessary kept up to date; 5. Personal data must be kept for no longer than is necessary; 6. Personal data must be processed in accordance with the rights of data subjects; 7. Appropriate technical and organisational measures must be established to protect the data; 8. Personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection.

196 NITDA Guidelines (n 194 above) 1.2.

197 NITDA Guidelines (n 194 above) 1.2.

198 Even some authors do not make reference to the Guidelines when considering the NITDA framework. Eg, Allotey (n 65 above) 127-128.

199 NIMC Act No 23 2007 available at http://resourcedat.com/wp-content/uploads/2013/03/National-Identity-Management-Commission-Act-2007.pdf (accessed 1 November 2015).

individuals, and the issuance of general multipurpose identity cards; and for related matters.'[200] The primary objective of NIMC is to 'establish and regulate a reliable and sustainable system of national identity management that enables a citizen or legal resident to assert his identity.'[201]

Obviously, a database contains personal information about individuals which will make data privacy laws applicable. This is more so for an institution like the NIMC whose primary work involves the collection,[202] storage and use of personal data. Data privacy issues that may arise from the NIMC's national identity database[203] include: processing of personal data for a specified purpose, accountability, security and safeguard of personal data in the database, data quality and data subject participation.

Regarding the processing of personal data for a specified purpose, there is no particular provision in the NIMC Act limiting processing for a particular purpose. However, it may

---

200 See the long title of the Act. See also sec 5. Specifically, sec 5(a) provides that the commission shall (a) create, manage, maintain and operate the national identity database established under sec 14 of this Act including the harmonization and integration of existing identification databases in government agencies and integrating them into the national identity database. The objectives of the database include to (a) use fingerprints and other biometric information as unique and unambiguous features of identifying registerable persons; (b) enable the Commission, using the information contained in the database to issue a multipurpose identity card with a unique identification number to registerable persons; (c) enable the harmonisation of existing identity card schemes in Nigeria; (d) provide a medium for the identification, verification and authentication of citizens of Nigeria and other registerable persons entitled to the multipurpose identity cards; (e) facilitate the provision of a secured and a reliable method for ascertaining, obtaining, maintaining and preserving information and facts about citizens of Nigeria and other registerable persons in accordance with the provisions of this Act, and whenever same is necessary or adjudged necessary in the public interest, providing such information to a designated and specified judicial or police authority; and (f) facilitate the provision of a convenient method for individuals who have been issued with the multipurpose identity cards to provide proof of facts entered about themselves in the database to other 'persons who reasonably require such proof. These objectives are explicitly stated to show the data privacy issues which a national identity database could raise.

201 See its vision statement in NIMC 'About us' https://www.nimc.gov.ng/?q=about-us (accessed 1 November 2015).

202 Sec 6(a) provides that the Commission has the power to 'request for any information on [sic] data from any person relating to its functions under this Act'. Eg of information to be collected include: the individual's full name; other names by which the person is or has been known; date of birth; place of birth; gender; the address of the individual's principal place of residence in Nigeria; the address of every other place in Nigeria where the individual has a place of residence; a photograph of the individual's head and shoulders; the individual's signature; the individual's fingerprints; other biometric information about the individual; the individual's residential status; the individual's national identity number; (to be issued by NIMC); any national insurance number allocated to the individual; any Nigerian or foreign passport number of the individual; (if available) driver's license number; (if available) record of any changes in the individual's recorded information; ID registration and history of such registration. See secs 17, 18 & 2nd Schedule of the Act. See also NIMC proposed Privacy Policy https://www.nimc.gov.ng/sites/default/files/pia_policy.pdf (accessed on 1 November 2015).

203 Sec 14(1) of the Act provides that 'there is hereby established a National Identity Database (in this Act, referred to as the "Database") which shall contain registered information or data relating to citizens of Nigeria and non-Nigerian Citizens who are registerable persons within the meaning of section 16 of this Act.'

be argued that the collection of personal information must be strictly towards realising the objectives of the Commission, which is contained in the long title of the NIMC Act and section 5.[204] Thus, any collection of personal data by the NIMC that is not for the purposes contained in the Act, especially section 5, is an unlawful collection. The issue of accountability of personal data in the national identity database is also crucial. There must be an official responsible to ensure that FIPs are complied with.[205] In this regard, there is no explicit provision in the NIMC Act. It is logical, however, to argue that the NIMC is accountable for all personal data in the national identity database. This is so because it is responsible for the general security and safeguard of personal data in its possession. Fortunately, the principle of safeguard and security of personal data is expressly provided for in the Act.[206] On the issue of data quality (accuracy of personal data), the Act provides that the Commission may verify any information supplied by a registered person from third parties.[207] Registered persons also have the right to request the correction and updating of personal information in the national database.[208] This is the NIMC Act's provision on data subject participation. Nowhere is it stated that a registered person should have access to the database for the purpose of viewing what is recorded about him/her. The NIMC Act seems to only make provision for updating of records and correction of error 'where he is aware'.[209] A registered person may not be aware of errors in his record unless he/she has access to what is recorded in the database. It may be argued that because information is collected from the individual directly, such errors are unlikely. But then, errors are errors and they can occur in the process of inputting details in the database. The right of access to information stored about an individual is a crucial aspect of data privacy law which should not be taken lightly.

The NIMC Act, compared to other Nigerian legislation and policies, has arguably provided for more rules on data privacy protection within its narrow scope of operation. This may be because of the large amount of personal data it handles. It is, however, observed that the

---

204 Sec 5 provides for the functions of the Commission.

205 Neethling (n 116 above) 247; see also Roos (n 88 above) 379-380.

206 Sec 5(g) provides that the Commission shall 'ensure the preservation, protection, sanctity and security (including cyber security) of any information or data collected, obtained, maintained or stored in respect of the National Identity Database'. See also sec 26 (1) which provides that no person or body corporate shall have access to personal data in the database except with the authorisation of the Commission and only if the person authorises or the individual consents.

207 NIMC Act, sec 20. See also sec 22(3) where the Commission may, for the purpose of verifying the updated personal information, require the registered person to attend at a specific place and time to provide further information.

208 NIMC Act, sec 22 generally.

209 NIMC Act, sec 22 (1).

Act does not provide for other critical aspects of a data privacy regime like special rules on sensitive personal data processing. Most of the data protection principles provided for are not explicitly stated in clear terms.

To ensure that the NIMC meets its obligations under the Act in the management of data in the database, the NIMC proposed a privacy policy.[210] The policy is designed to safeguard the privacy of registered persons by ensuring the security of the information collected in the database, guarding against unauthorised disclosures, ensuring that information is used only for the purpose for which it is collected and personal information is not disclosed or used except in the interest of national security and that it is preceded by the consent of the individual.[211] For these purposes, the policy applies to all NIMC employees, registered information and 'any other person or third party as may from time to time be designated by NIMC.'[212] The extent to which this policy has helped in personal data protection within the NIMC is uncertain. However, it is possible that such policy has not been given the requisite publicity especially among NIMC employees.

The NIMC has made further efforts on data privacy protection by pushing for the enactment of a general legislation on data privacy. It proposed a Bill on Personal Information and Data Protection.[213] The Bill is yet to be tabled before the legislature in Nigeria.

3.6.4. Other Institutions

A number of other institutions that process individuals' data in Nigeria lack legal frameworks for data privacy protection.[214] They merely have soft laws (regulations and guidelines) which regulate the processing of personal data by themselves and by the entities they regulate. [215] As was previously argued, regulations and guidelines are far weaker with lesser binding force than legislation. Moreover, there is little or no evidence to show that these institutions take extra steps to enforce the provisions of these soft laws. For example, while there are reports that the NCC fined some telecom providers for poor

---

210 NIMC Proposed Privacy Policy available at https://www.nimc.gov.ng/sites/default/files/pia_policy.pdf (accessed 1 November 2015).
211 NIMC Proposed Privacy Policy, at 2.
212 NIMC Proposed Privacy Policy, at 3.
213 'Nigeria: Adoke lauds NIMC Proposed Draft Bill on Information, Data Protection' http://allafrica.com/stories/201302220301.html (accessed 1 November 2015).
214 The main laws regulating these institutions do not also have provisions protecting data privacy.
215 Eg, the CBN Guidelines for Licensing, Operations and Regulation of Credit Bureaus in Nigeria, Sec 5.7

service delivery, there is little evidence suggesting that any service provider has been punished for violation of data privacy and such occurs on a regular basis.[216]

3.6.5. The Courts

The courts have a responsibility to protect data privacy as they are usually accorded the key role of interpreting and enforcing statutory norms.[217] According to Bygrave, in common law jurisdictions, courts play a key role in developing norms outside statute.[218] However, this is not the case in Nigeria as there is no judicial pronouncement on the data privacy protection. This is not surprising because there are no coherent policies and legislation on data privacy protection in Nigeria. Even the right to privacy which debatably underpins data privacy has hardly been pronounced upon by the courts in Nigeria.[219] To the best of this researcher's knowledge, no issue on data privacy has featured in a case law in Nigeria.[220] Allotey identifies three reasons for the absence of case law on information privacy particularly and privacy in general. The first reason identified is the weak notion of privacy. According to the author, the notion of privacy is weak in the African understanding of human rights.[221] The second reason is the limited exposure to telecommunication facilities. The high poverty level is the third reason advanced by Allotey.[222] This researcher disagrees with the second reason put forward by Allotey. The level of exposure to telecommunication facilities in Nigeria used to be extremely limited. It is submitted, however, that the situation has drastically changed in recent times. The telecommunications industry and the concomitant exposure of the Nigerian people to ICTs have significantly developed within the last few years. Thus, the people and the courts are supposed to seize this opportunity to enhance the jurisprudence on data privacy in Nigeria. Probably with the FOIA and the excitement that comes with it, an issue involving data privacy may sooner than later come before the court. One awaits such development in Nigeria's jurisprudence.

---

216 'NCC fines four GSM operators N1bn' *The Punch Newspaper* 13 May 2012. http://www.punchng.com/news/poor-services-ncc-fines-four-gsm-operators-n1bn/ (accessed 1 November 2015).

217 LA Bygrave *Data privacy law: An international perspective* (2014)179.

218 Bygrave (n 217 above) 179.

219 Nwauche (n 68 above) 66, Allotey (n 65 above) 188.

220 Allotey shares a similar view. (n 55 above) 188.

221 Allotey (n 65 above) 188.

222 Allotey (n 65 above) 191.

3.7. Review of legislative efforts on data privacy protection in Nigeria: An analysis of the challenges for effective protection of personal data

The forgoing sections of the chapter have shown that there is an absence of coherent policies on data privacy protection in Nigeria. The legislative framework is limited and the institutional framework is inadequate. This is not without consequences for the Nigerian society in the digital age. Nevertheless, there have been some attempts on the part of the Nigerian legislature towards data privacy protection. These attempts are in the form of bills on privacy and/or data protection and related matters. The first effort made by the Nigerian legislature was in 2005 with a Bill for an Act to provide for Computer Security and Critical Information Infrastructure Protection.[223] This was followed by the Cyber Security and Data Protection Agency Bill 2008[224] and the Electronic Fraud Prohibition Bill 2008.[225] In 2009, two attempts were made with the Nigeria Computer Security and Protection Agency Bill[226] and Computer Misuse Bill.[227] In 2010, there was the Economic and Financial Crimes Commission Act (Amendment) Bill 2010 and the Cyber Security and Information Protection Agency Bill 2012 which has gone through a second reading.[228] It is important to state that all these Bills are not specifically on data privacy protection. Most of them focus on combating ICT crimes and related issues. As a consequence, they have very scanty provisions on data privacy protection.[229] Another observation regarding these Bills is that they focus on the protection of data generally as a way of combating cybercrimes, rather than on data privacy protection specifically. Thus, a Bill on data privacy protection should be the primary focus of this section.

---

223 Available at http://www.nassnig.org/nass/legislation.php?id=103 (accessed 1 December 2014).
224 Available at http://www.nassnig.org/nass2/legislation.php?id=410 (accessed 1 December 2014).
225 Available at http://www.nassnig.org/nass/legislation.php?id=349 (accessed 1 December 2014).
226 Available at http://www.nassnig.org/nass2/legislation.php?id=410 (accessed 1 December 2014).
227 Available at http://www.nassnig.org/nass/legislation.php?id=724 (accessed 1 December 2014).
228 T Kio-Lawson 'The right to be forgotten' *Business Day* 1 June 2014 available at http://businessdayonline.com/2014/06/right-to-be-forgotten/#.VF5UKjTF9yJ (accessed 1 November 2015).
229 Eg, the Cyber Security and Data Protection Agency (Establishment) Bill 2008 has just a section that relates to personal data protection. Sec 17(d) provides that 'every service provider shall ensure that any of its equipment, facilities or services that provide communication is capable of facilitating authorised interceptions and access to call data or traffic records with minimum interference with any subscriber's communication service and in a manner that *protects the privacy and security of communications and call data or traffic*.' (Emphasis added).

In 2009, there were efforts to pass a law directly on data privacy protection with the Privacy Bill of 2009.[230] It was followed shortly by the Data Protection Bill in 2010.[231] Recently, the Personal Information and Data Protection Bill was also drafted.[232] None of these Bills have been passed into law as attempts to do so have always been met with hurdles.[233] This points to the neglect of data privacy protection by the Nigerian government.

For the purpose of this section, the Data Protection Bill 2010 and Personal Information and Data Protection Bill 2012 will be analysed. Both draft Bills are the most recent efforts by the Nigerian legislature and they are the closest initiatives towards an omnibus data privacy law in Nigeria.[234] An examination of these Bills will be carried out with a view to identifying their various challenges and predict how effective they may be should any of them be eventually enacted as law. Salient features of the provisions of the draft Bills will be analysed within the context of the basic features of a data privacy regime or legislation which are:

I. Scope of the law
II. Conditions for personal data processing/FIPs
III. Rights of data subject and duties of data controllers
IV. Exemptions and qualifications
V. Supervision and enforcement
VI. Requirement of transborder flow of personal data

---

230 http://www.nassnig.org/nass2/legislation2.php?search=privacy&Submit=Search (accessed 1 November 2015).

231 http://www.nassnig.org/nass2/legislation2.php?search=data+protection&Submit=Search(accessed 1 November 2015).

232 The exact status of this Bill is unknown.

233 Kio Lawson (n 228 above).

234 Arguably, the Privacy Bill of 2009 also envisages data privacy protection even though it does not make use of the term 'data protection' or 'data privacy'. Sec 1 of the Bill limits its application to only the government and its agencies. Also, the Bill pays too much attention to access to information rather than data protection (Part V of the Bill). The conditions for lawful processing of personal data are not explicitly stated as is the case in many international codes on data protection. The Bill also grants the government significant powers and exemptions for personal data processing. (See Part VI). It must, however, be pointed out that the Bill contains provisions on a supervisory agency unlike the Data Protection Bill (See part IX). However, the requirement of independence of the data protection authority is absent in the Bill. Sec 48 which establishes the Privacy Directorate requires that the directorate should be established in the office of the federal ministry of justice which is component of the executive arm of government. One therefore wonders how the privacy directorate, that is an arm of the government, can sanction it for illegal or wrongful data processing activities.

3.7.1. Data Protection Bill 2010

The Data Protection Bill[235] is before the Nigerian National Assembly.[236] Its primary objective is to 'provide for personal data protection to regulate the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information and for related matters.'[237] This objective of the Bill is couched in a rather confusing manner. The long title of the Bill makes it seem as if the primary objective of personal data protection is to regulate the processing of information relating to individuals when the reverse should be the case. Basic principles of the law on data privacy show that data privacy protection is achieved through the regulation of the processing of personal information. Consequently, a law on data privacy should 'regulate the processing of information' so as to 'provide for personal data protection' and not the other way round.[238] Moreover, the object of the law as provided in the Bill is too vague.

3.7.1.1. Scope of the law

The Bill does not provide for the entities that will be bound by its provision which is very abnormal for a typical law on data privacy. In many circumstances, a law of this nature provides that it is applicable to public or private data controllers or both. The definition of a data controller in the interpretation section states that a data controller is 'person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which only personal data are, to be processed.'[239] This definition does not specify the scope in terms of persons. It is, however, plausible to argue that since the Bill does not specifically exclude any category of person, then it is applicable to both private and public entities. Such contention is, however, a mere speculation.[240]

Regarding the category of activities that will be covered by the Bill, it is stated that it covers 'the processing of information relating to individuals, including the obtaining,

---

235 Sec 11.

236 See G Greenleaf 'Global tables of data privacy laws and bills' (3rd ed, June 2013). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875 (accessed 1 November 2015).

237 Long title of the Bill

238 A statement in the explanatory memorandum seems more apt for the object of the Bill. It is stated that 'this Bill seeks to make provision for the regulation of the processing of information relating to individuals'

239 Data Protection Bill 2009, sec. 10.

240 The explanatory memorandum of the draft Bill contains little or nothing which would have been helpful in such controversies regarding interpretation.

holding, use or disclosure of such information and for related matters.'[241] Thus, the Bill covers any processing of information relating to individuals. Some examples of activities of processing, as stated in the long title, include obtaining, holding, use or disclosure. However, it is submitted that the list is not exhaustive. Processing of personal data as defined in the draft Bill

> …means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-
> a. Organisation, adaptation or alteration of the information or data,
> b. Retrieval, consultation or use of the information or data,
> c. Disclosure of the information or data by transmission, dissemination or otherwise making available, or
> d. Alignment, combination, blocking, erasure or destruction of the information or data.

The Bill further defines 'obtaining' or 'recording' to include 'obtaining or recording the information to be contained in the data'.[242] 'Using' or 'disclosing' on the other hand means 'using or disclosing the information contained in the data.'[243] It is submitted that these definitions are not definitions at all as they do not tell us what their meanings are and how they constitute processing of personal data.

The Bill does not expressly state if it is applicable to both manual and automated processing, however; based on the definition of data in the interpretation section, its scope seems to cover both manual and automated processing.[244]

3.7.1.2. Conditions for personal data processing/FIPs

The Data Protection Bill, unlike many other data protection legislation, does not expressly provide for the conditions for lawful processing. The FIPs are not contained anywhere in the Bill. This brings about confusion as the *raison d'etre* of the law on data privacy is to permit processing of individuals personal data if certain conditions are followed. The question therefore arises as to whether the Bill intends to prohibit information processing completely, which is antithetical to the philosophy of data privacy law.

---

241 See the long title of the Bill.
242 Sec 10.
243 Sec 10.
244 See sec 10 which defines data as information being processed by means of equipment operating automatically or recorded with the intention that it should be processed by such equipment or '*recorded as part of a relevant filing system or with intention that it should form part of a relevant filing system'* (Emphasis added).

Section 1 of the draft Bill, however, provides for rules on 'handling of personal data.' One may therefore argue that conditions for the handling of personal data may also be interpreted to mean conditions for the processing of data as 'processing' means all activities which is performed on personal data. In the same vein, 'handling' may also be said to be any activity performed on personal data.

The Bill provides for the processing limitation and purpose specification principles. It requires that personal data shall be processed fairly and lawfully and must be obtained for one or more specified and lawful purposes.[245] It is further provided that personal data shall not be further processed in any manner incompatible with that purpose or purposes.[246] The essential details of what constitutes these principles are not, however, stated in the Bill. For example, it is not stated if the processing limitation principle limits data controllers in the amount of personal data collected to what is necessary to achieve the purpose(s) for which the data is processed.[247] Other details such as the fact that personal data must be collected from the data subject are similarly not contained in the Bill.

In terms of the Bill, personal data should be adequate, relevant and not excessive;[248] it must also be accurate and kept up to date where necessary.[249] These are the Bill's provision on the requirement of information quality. The safeguard principle also seems to have been provided for in the Bill. It is stated that: '[a]ppropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'[250] Certain issues, however, arise regarding the provision. The Bill does not state who should take 'appropriate technical and organisational measures.' In many cases, it may be argued that it is the sole responsibility of the data controller. However, it must be noted that in some instances, personal data is not being processed by the data controller himself. There are cases where a third party processes personal data on behalf of the data controller. This

245 Sec 1(1)(a) & (b).
246 Sec 1(1) (b).
247 Usually referred to as the principle of minimality. Roos (n 88 above) 371; Eg, a school that collects data from a prospective candidate for the purpose of admission. Such collection must be limited to personal data of the candidate necessary for acceptance into the school. Other personal data such as the prospective candidate's shopping habit or sex life, which is not necessary for the purpose of admission, must not be collected by the data controller.
248 Sec 1 (1) (c).
249 Sec 1 (1) (d).
250 Sec 1 (3).

imprecise provision may therefore bring about confusion. This is as far as the Bill goes in providing for data protection principles.

3.7.1.3. Rights of data subjects and duties of data controllers

In terms of the Bill, personal data should be 'processed in accordance with the rights of the data subjects.'[251] The Bill makes provision for a number of data subject rights.

a. The right of access to personal data

The Bill provides that a data subject is entitled to be informed by a data controller if his/her personal data is being processed.[252] He/she is to be given a description of the personal data, the purpose of processing and the possible recipients of the personal data.[253] A data subject is also entitled to be communicated to in an intelligible form, the information constituting personal data of the data subject and any information which forms the source of those personal data.[254]

In the case of processing by automated means for the purpose of evaluating matters relating to him/her, the data subject is to be informed of the logic of the decision making.[255] There are, however, cases where a data controller is entitled to deny a request for access to personal information. Such instances include where the request is not made in the prescribed form or where the necessary fees have not been paid.[256] Also, a request may be denied unless the data subject supplies such information as the data controller may reasonably require in order to satisfy himself/herself as to the identity of the person making the request and to locate the information being requested.[257] If a data controller cannot supply the requested information without disclosing personal information of another individual, the data controller may deny the request for access.[258]

---

251 Sec 1(1) (e).

252 Sec 2(1)(a). This subsec is one of the numerous cases of bad draft style as it provides that 'an individual is entitled where such individual is a data subject…' The provision makes it seems as if there are cases where an individual is not a data subject and is still being protected by the provisions of the Bill.

253 Sec (2)(b) i-iii.

254 Sec (2)(c).

255 Sec (2)(d).

256 Sec 2(2).

257 Sec 2(3).

258 Sec 2(4). There are exceptions which include where that other individual consents or where it is reasonable in the circumstance to comply with the request without consent.

b. Right to prevent processing likely to cause damage or distress

A data subject is entitled, by notice in writing, to require the data controller to end processing, or not to begin processing for a specified purpose or in a specified manner, on the ground that it is likely to cause 'substantial damage' or 'substantial distress'[259] and the damage or distress is or would be unwarranted.[260] This right is uncommon in data privacy laws as it may be argued that one of the reasons for regulating processing of personal data is so as to prevent processing likely to cause damage or distress. It therefore becomes superfluous to set out a specific provision for this purpose. This makes this provision very difficult to comprehend. The vague provision does not help matters as it does not specify the meaning and/or examples of processing 'likely to cause substantial damage or distress.' Perhaps the right is meant to provide for processing of sensitive personal data. However, this cannot be confidently stated to be the intention of the law makers.[261]

c. Right to prevent processing for purposes of direct marketing

Like many other laws on data privacy, the Data Protection Bill also provides that a data subject may, by notice in writing, require the data controller to cease or not to begin processing for purposes of direct marketing.[262] Direct marketing, according to the provision is 'a communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.'[263]

d. Rights in relation to automated decision taking

A data subject has a right to prevent the data controller (or his/her representative) from taking any decision which significantly affects him/her based solely on processing by

259 Sec 3 (1) (a).
260 Sec 3 (1) (b).
261 The South African Protection of Personal information Act (POPIA) of South Africa seems to contain a similar provision. Sec 11(3)(a) provides for a right to object to certain processing activities stipulated under the Act. However, a distinction can be maintained between the Nigerian Data Protection Bill and the POPIA in that the latter only grants rights to object in cases of processing under sec 11 (1)(d)-(f) and for direct marketing or unsolicited electronic communication purposes. This is unlike the Data Protection Bill that grants a general right to object on the grounds of likelihood to cause substantial damage or distress.
262 Sec 4 (1).
263 Sec 4 (3).

automated means.[264] Such decisions include decisions evaluating matters relating to the data subjects' work performance, creditworthiness reliability or conduct.[265]

e. The rights to rectification, blocking, erasure and destruction

A data subject has the right to apply to the court to have inaccurate personal information being processed by the data controller to be rectified, blocked, erased or destroyed. If the court is satisfied on the application of the data subject, it may order the data controller 'to rectify, block, erase or destroy' the data.[266] This provision extends to any other personal data in possession of the data controller which contains an expression of opinion and which appears to the court to be based on the inaccurate data being process.[267] Application to the court for rectification can be identified as one of the areas of weakness of the Bill as involvement of the court in this regard may be expensive for aggrieved parties.

For each of the forgoing rights bestowed on the data subject, it is argued that there is a corresponding duty on the data controller to respect such right. For example, with regard to the right of access, the data controller has a duty to inform the data subject where his/her personal data is being processed.[268] A data controller also owes the data subject a duty of confidentiality.[269]

3.7.1.4. Supervision and enforcement

The Data Protection Bill is unique in that it does not provide for a particular body (Data Protection Authority) responsible for supervision or enforcement of the provisions of the Bill.[270] It merely provides, in some instances, for the court to perform certain roles.[271] It is therefore arguable that the court is responsible for the supervision and enforcement of the provisions of the Bill. Certain issues may arise as the Bill does not specify the particular court referred to and its jurisdiction.[272] Also, the courts are merely to intervene in

---

264 Sec 5 (1).
265 Sec 5(1)
266 Sec 7(1).
267 Sec 7(1).
268 Sec 2 (1).
269 Sec 2 (7) (a).
270 AB Makulilo 'Nigeria's Data Protection Bill: Too many surprises' (2012) 120 *Privacy Law and Business International Report* 26
271 See eg, sec 2(10); 4(2); 5 (5); 7 (1); 8(2) & (3)649(3)(a).
272 Makulilo (n 270 above) 26.

particular circumstances which means beyond those circumstances,[273] the courts do not have jurisdiction to interfere in violations of data privacy.

The main remedies which are provided for by the Bill are injunction, compensation and criminal offences. With respect to injunctions, the court has powers to make an order for compliance in many cases.[274] In terms of section 6 of the Bill, an individual (data subject) is entitled to compensation for the data controller's failure to comply with certain requirements of the Bill. This is so where the individual has suffered damage or distress.[275] From the provisions of section 6 of the Bill, it seems liability of the data controller only arises when there is fault.[276] Certain criminal sanctions also follow violation of some provisions in the Bill. For example, it is an offence to knowingly or recklessly obtain and disclose personal data without the consent of the data controller.[277] Similarly, a person who sells personal data obtained knowingly and recklessly is guilty of an offence.[278] The Bill's provision on offences is problematic for two reasons. First, it is surprising that all provisions creating offences do not provide for punishment for such offence. Related to the first problem is that the provisions on offences may amount to 'a dead-letter law' as the Nigerian Constitution provides that:

> …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.[279] [Emphasis added].

From the above provision, no person can be charged with an offence under the provisions of the Bill.

---

273 Makulilo (n 270 above) 26.

274 See eg, Data Protection Bill, sec 2(10) where the court can order a data controller to comply with a request for access to personal data; sec 4 (2) where the court, on application of the data subject, can make an order for complying with notice requiring ending processing of personal data for direct marketing purpose etc.

275 Secs 6 (1) & (2).

276 Unlike the South African POPIA where liability is faultless.

277 Sec 8(1) & (3).

278 Sec 8(4). Other provisions of the Bill which provides for criminal sanctions include sec 8(5) & 9(4).

279 Sec 36 (12) of the Constitution. See also the case of *Aoko v. Fabgemi* (1961) 1 All NLR 400. See also IKE Oraegbunam 'Crime and punishment in Igbo Customary Law: The challenge of Nigerian criminal jurisprudence' (2010) 6 (1) *New Journal of African Studies* 53-85.

3.7.1.5. Requirement of transborder flow of personal data

Like the prevailing trend in legislating for data privacy protection, the Bill contains a provision which restricts the flow of personal information outside the territories of Nigeria, unless that country or territory ensures an adequate level of protection of personal data.[280] This is a welcomed feature of the Bill; however, the provision raises issues such as the means or methodology of assessing 'adequate level of protection' and the penalty for failure to comply with the Act. The Bill, furthermore, does not provide for situations where data can be transferred to a country or territory without an adequate level of data protection when certain other conditions prevail, as is the case in many other modern data privacy laws.[281]

3.7.2. A critique of the Data Protection Bill 2010

The Bill has shown that the Nigerian legislature is making some efforts to move towards data privacy protection. It makes provision for a number of rights to enhance individuals' control over their personal data, some of which only recently featured in data privacy laws.[282] Nevertheless, the Bill, in its present form, raises many issues which have been a basis for criticisms. For example, some basic principles of data protection (FIPs) are missing in the Bill. Makulilo observes that the principles contained in the Bill fall sort of international standards on data protection.[283] He further contends that 'to make matters worse, the draft Bill does not contain conditions for legitimate processing…'[284] In other words, the draft Bill does not outline criteria for making data processing legitimate which makes one wonder if it altogether prohibits the processing of personal data.[285] Another manifest omission is that the Bill does not contain any provision which protects sensitive personal data (yet, somewhat contradictory, it defines sensitive personal data in the interpretation section).[286] This is rather surprising for a Bill that purports to regulate the processing of information. Furthermore, there is no provision for a supervisory authority,

280 Sec 1 (4).
281 Makulilo (n 270 above) 26. See for eg, art 26 of the EU Directive.
282 Eg, right to erasure, deletion and blockage.
283 Makulilo (n 270 above) 26.
284 Makulilo (n 270 above) 26.
285 Eg, art 7 of the EU Directive provides for instances where processing is legitimate. It is provided that processing is legitimate where the data subject consents, where processing is necessary for compliance with a legal obligation, where processing is necessary in order to protect the vital interest of the data subject and where processing is necessary.
286 See sec 10. It was observed that 'some important terminologies and phrases remain undefined. Similarly, there are terminologies and phrases which although defined in the interpretation section, are not found within the text of the Bill.' Makulilo (n 270 above) 25.

usually a Data Protection Authority/Agency (DPA). The responsibility of supervising compliance with the Bill seems to fall on the courts. This is problematic in that it is generally known that the courts do not act *suo moto*. For the powers of the courts to be activated, there must be a positive act by a party. What this implies is that no particular agency actively monitors the implementation of the Bill.

Enforcement of the provisions of the Bill will appear to be a mirage because many of its provisions are vague and ambiguous; this should not be the case for a law that creates rights for the people. The draft Bill does not contain serious penalties for violation of its provision. It merely creates offences without stipulating punishments which run afoul of the Constitution. The Bill also contains areas of weak use of language and poor arrangement style.[287]

A proposed law of this nature, which establishes relatively novel rights, ought to be clear and authoritative. However, the Bill in its present form presents a weak standard of data protection legislation.[288] Makulilo specifically states that in the event the Bill is enacted without substantial modifications, the Nigerian law will undermine the cross jurisdictional transfer of personal data in Africa.[289]

3.7.3. Personal Information and Data Protection Bill 2012

The Personal Information and Data Protection Bill 2012[290] is the most recent legislative effort on data privacy protection in Nigeria. The Bill was drafted by the NIMC as part of its initiatives towards data privacy protection in Nigeria.[291] The exact status of the draft Bill, however, remains uncertain as there is no evidence that it has been tabled before the Nigerian Legislative Assembly.[292] The Bill has two broad objectives. It seeks to provide for rules governing the processing of personal information 'in a manner that recognizes the right to privacy of individuals with respect to their personal information' and also the need

287 Eg, there are some omissions in the arrangement of the secs and subsecs. Secs 2(2)(5) and 5(3) are omitted.

288 Makulilo (n 270 above) 27.

289 Makulilo (n 270 above) 27.

290 A copy of the Bill is on file with the researcher. The Bill is not available on the National Assembly website.

291 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 1 November 2015).

292 This is because it is not on the Nigerian National Assembly's website. See http://www.nassnig.org/nass2/legislation.php and http://www.nassnig.org/nass/legislation.php (1 November 2015).

for organisations to process personal data for purposes that a reasonable person will consider appropriate.[293]

3.7.3.1. Scope of the Bill

The Bill applies to every person and organisation that collects, uses or discloses personal data in the course of its commercial activities.[294] The Bill is also applicable to the processing of personal information of an employee of an organisation whose operation is in connection with a federal work, undertaking or business.[295] The Bill does not, however, apply to any government institution, or the processing of personal data for personal and domestic purposes.[296] An organisation that processes personal data for journalistic, artistic or literary purposes is also completely outside the scope of the Bill.[297]

3.7.3.2. Conditions for personal data processing/FIPs

In a rather strange fashion, the body of the draft Bill does not contain the FIPs.[298] However, section 3 provides that 'every organization shall comply with obligations set out in Schedule 1.' Schedule 1 contains 'privacy principles for the protection of personal information.' Principle 1 is on accountability, it holds an organisation responsible for personal information under its control. The principle also requires that an organisation designate an individual responsible for implementing the principles.[299] Principle 2 is on identifying purpose. An organisation must specify the purpose for data collection before or at the time of collection.[300] Principle 3 provides that the knowledge and consent of the individual whose data is collected is required except in certain specified circumstances.[301] Principle 4 limits collection of personal data to that which is necessary for purposes identified by the organisation. Principle 5 restricts use, disclosure and retention of personal data. Principle 6 is the equivalent of information quality principle. It requires organisations

---

293 Protection Information and Data Protection Bill, sec 1.

294 Sec 2(1)(a). Commercial activity means 'any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.' From this definition, churches, schools or political parties, even though not strictly profit making ventures, may be covered by the act if they carry out any transaction that of commercial character.

295 Sec 2(1)(b).

296 Sec 2(2)(a) & (b).

297 Sec 2(2)(c).

298 Some data privacy legislation adopt this style eg the UK Data Protection Act 1998 and the Canadian Protection of Personal Information and Electronic Documents Act (PIPEDA) 2001.

299 Schedule 1; 4.1.

300 Schedule 1; 4.2.

301 Eg, for legal, medical or security reasons.

to ensure that personal information is 'accurate, complete and up-to-date' for the required purpose. The security safeguard of personal information is contained in principle 7. Principle 8 requires openness regarding policies and practices of management of personal data by an organisation. Principle 9 grants individuals access to their personal data upon request. Special recognition is given to people with sensory disability and access may be granted in an alternative format.[302] Finally, the right to challenge compliance with the principles is granted to individuals and it is contained in principle 10. Part 2 of the Bill contains a series of remedies and enforcement options for individuals. Also contained in part 2 are provisions on a DPA.

3.7.3.3. Rights of data subjects and duties of data controllers

Unlike many data privacy codes, the draft Bill does not provide for the rights of data subjects and obligation of data controllers. These can, however, be deciphered from the principles of data processing discussed above.

3.7.3.4. Supervision and enforcement

Section 4.1 establishes the Office of the Privacy Commissioner who 'shall be responsible for implementation and administration of the Act.'[303] The Privacy Commissioner is the head of the office.[304] The functions of the Commissioner are contained in the Bill and it includes promotion of awareness and understanding of the provisions of the Act, especially the data protection principles.[305] This function is indeed crucial for Nigeria. The Bill does not, however, provide for the requirement of independence of the Privacy Commissioner which is a basic requirement in international data protection codes.[306]

3.7.3.5. Requirement of transborder flow of personal data

The draft Bill does not contain any provision which restricts the transborder flow of personal information to a third country without an adequate level of personal data protection.

---

302 Sec 9.
303 Sec 4.1 (7).
304 Sec 4.1 (2).
305 Sec 4.4 (c).
306 See G Greenleaf 'Independence of data privacy authorities (part I): International standards' (2012) 28 *Computer Law & Security Review* 3-13.

3.7.4. A critique of the Personal Information and Data Protection Bill 2012

The Bill contains some innovations which may enhance effective data protection. For example, the Bill provides a platform for the Privacy Commissioner to collaborate with states for effective personal data protection.[307] This is crucial for data privacy protection in a large country like Nigeria. It also has a special provision which focuses on the role of the Commissioner in promoting the purpose of the Act.[308] The Bill protects whistle-blowers on data privacy related issues.[309] Periodic review of the administration of the Bill is also provided for.[310] The Bill contains FIPs which are largely similar to what is provided for in the EU Directive. However, these principles are contained in the schedule of the law which has drawn criticisms.[311]

It must be pointed out that it may take a really long time for a Bill of this kind to be enacted as law.[312] Moreover, the relationship between the present Bill and the Data Protection Bill is still uncertain. Questions may arise as to which of them takes precedent. This goes to show the multiplicity of policies in Nigeria which brings about confusion and poor implementation. The Personal Information and Data Protection Bill, like its predecessor (the Data Protection Bill), also has some apparent shortcomings. The exclusion of data processing activities by the government from the provisions of the Bill has drawn intense criticism.[313] There are also instances of clear omissions in the Bill. For example, there is no regime on sensitive personal data.[314] Transborder data flow, with its

---

307 See sec 24.

308 Sec 26.

309 Sec 29.

310 Sec 32.

311 Article 19 (an NGO) for example states that 'of primary concern is that the basic principles that govern the law have been subjected to a schedule in the back of the law rather than in the main text. This approach requires a back and forth reading of the law which has been inconsistently applied.' Article 19 'Nigeria Personal Information and Data Protection Bill' (2013) available at http://www.article19.org/resources.php/resource/3683/en/nigeria:-personal-information-and-data-protection-bill (accessed on 1 November 2015) 8.

312 The FOIA took a period of 12 years before in the Nigerian legislative assembly before it was passed as law. See F Waziri 'Freedom of Information Act 2011; Comparative study with the United State Freedom of Information Act of 1966' in Waziri & Azinge E Azinge & F Waziri (eds) *Freedom of information law & regulation in Nigeria* (2012) 69.

313 See Article 19 (n 311 above) 8.

314 Sec 4.3.4 of schedule 1 seems to provide for sensitive personal data. In stipulating that the consent of the individual must be sought for the processing of his/her personal data, the section provides that 'the form of the consent sought by the organisation may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organisations shall take into account the sensitivity of the information. Although some information (eg, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context.' Similarly, sec 4.7.3 of Schedule 1 in providing for the safeguard principle requires that '[t]he nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the

attendant risks, is not regulated in any form. This means that the personal data of Nigerians can move freely to other jurisdictions without any form of protection. If the Bill is enacted in its present form, it will obviously not meet the adequacy requirement of the EU Directive. The Bill emphasises more on procedural issues and treats substantive matters rather casually. The definition of personal information adopted in the Bill is extremely limited as it does not protect personal data of employees of an organisation.[315] It is submitted that this is discriminatory. The whole definition section is very scanty. Like the Data Protection Bill, the Personal Information and Data Protection Bill is poorly drafted and contain numerous cases of conflicts.[316]

An apparent weakness of the Bill is that the proposed Privacy Commissioner only has powers to make recommendations and individuals whose rights have been violated must seek redress in the Federal High Court.[317] If the Bill eventually makes it to National Assembly and is passed into law in this form, its ability to influence the desired level of data privacy protection will be very limited.[318]

3.8. Regional and sub-regional initiatives on the protection of data privacy and the extent of influences in Nigeria

From the forgoing analysis, adequate data privacy protection in Nigeria is far from being attained at the national level. The laws have extremely narrow provisions and the institutional framework is inadequate. Attention may therefore be turned to regional and sub-regional instruments with a view to seeing how (if at all) they have influenced data privacy protection in Nigeria.[319] The discussion will not be in detail, since an elaborate analysis of these instruments is outside the scope of the chapter.[320]

---

amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in clause 4.3.4.'

315 Sec 33 defines personal information as 'information about an identifiable individual, *but does not include the name, title or business address or telephone number of an employee of an organization.'* (Emphasis added).

316 Article 19 (n 311 above) 8. See eg, sec 30.

317 See sec 8(3)(b); Article 19 (n 311 above), 11 &16.

318 It has been pointed out that '…overall the bill is poorly drafted and confusing. It is inconsistent in major ways with the international legal obligations on Nigeria to adequately protect the privacy rights of its citizens, especially as set out by the ECOWAS. It also threatens freedom of expression rights.' Article 19 (n 311 above) 2.

319 This is also important because art. 25(6) of the EU Directive provides that 'the commission may find…that a third county ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of *the international commitments* it has entered into … for

Nigeria is an active (and one of the founding) members of the African Union (AU).[321] It is also located in the West African sub-region, hence, a state party of the Economic Community of West African States (ECOWAS). Both regional institutions have responded to threats resulting from personal data proliferation and processing with some legal instruments which will now be briefly considered.

3.8.1. African Union's (AU) initiatives: African Union Convention on Cyber-security and Personal Data Protection

Some initiatives have been carried out in the African region regarding data privacy;[322] however, focus is herein placed on the initiatives by the AU. The ACHPR has no provision on the right to privacy, yet the AU recognised the importance of data privacy protection. The first initiative of the AU was in 2011 with the issuance of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security.[323] A second draft, albeit with a slight name modification, was issued in 2013. It is titled the African Union Convention on the Confidence and Security in Cyberspace. Both instruments, however, focused on cyber security with scanty provisions on data privacy protection.

A further initiative towards data privacy protection by the AU was the adoption of the African Union Convention on Cyber-security and Personal Data Protection ('AU Convention' or 'the Convention') on the 27th of June 2014.[324] This is said to be the most important development on data privacy in Africa.[325] Thus, Africa is the first continent

---

the protection of private lives and basic freedoms and rights of individuals.' (Emphasis added). It is submitted that international commitments referred to in this provision also include regional and sub-regional obligations.

320 For more analysis, see G Greenleaf & M Georges 'The African Union's Data Privacy Convention: A major step toward global consistency?' (2014) 131 *Privacy Laws & Business International Report*, 18-21.

321 Formerly, the Organization of African Unity (OAU).

322 Eg, the African Declaration on Internet Rights and Freedoms which was launched by a group of 21 civil society organisations working on internet governance in Africa. Highlights of the declaration include demand for protection of privacy and data security. The declaration was presented at the African Union Conference of Ministers in charge of Communication and Information Technologies which took place in the first quarter of 2015. http://africaninternetrights.org/about/ (accessed 1 November 2015).

323 Available at http://www.au.int/en/sites/default/files/AU%20Convention%20EN.%20%283-9-2012%29%20clean_0.pdf (accessed on 1 November 2015). AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 81.

324 This was at the AU submit in Malabo, Equatorial Guinea. The Convention is available online in http://pages.au.int/sites/default/files/AU%20Cybersecurity%20Convention%20ENGLISH_0.pdf (accessed 1 November 2015).

325 See Greenleaf & Georges (n 320 above).

outside Europe to adopt a Data Protection Convention as a matter of international law.[326] The Convention has more potential state parties than any other international data privacy agreement.[327]

The Convention (with provisions on cyber-security) has a chapter on data protection.[328] It commits state parties to establish a legal framework for strengthening fundamental rights and public freedom with particular emphasis on physical data.[329] It also penalises any violation of privacy without prejudice to free flow of personal data.[330] The Convention does not define 'physical data' although one may argue that it has the same meaning as personal data under the EU Directive.[331]

3.8.1.1 Scope: The Convention applies to any processing of personal data carried out in the territory of a state party.[332] A state party is a member state who has ratified or acceded to the Convention.[333] The Convention covers the processing of personal data by natural persons, state, local communities and public or private bodies.[334] It also covers automated and manual processing.[335]

3.8.1.2 Principles of data processing: Articles 13 to 23 set out the main principles on personal data processing which are similar to the approach adopted by the EU Directive.[336] The Convention encourages state parties to prohibit any processing of sensitive data, but

---

326 Greenleaf & Georges (n 320 above).

327 The Council of Europe Convention 108 is the European International data privacy framework. It has only been ratified by 46 countries and one accession. The AU on the other hand has 54 states. See Greenleaf & Georges (n 320 above).

328 Chapter 2.

329 Art 8.

330 Art 8.

331 Art. 2 of the EU Directive defines personal data as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'

332 Art 9 (1) (d).

333 Art 1.

334 Art 9 (1) (a).

335 Art 9 (1) (b).

336 Principle 1 is principle of consent and legitimacy of personal data processing; principle 2 is on lawfulness and fairness of personal data processing; Principle 3 provides for purpose, relevance and storage of processed personal data, principle 4 is for accuracy of personal data, principles 5 and 6 are on transparency of data processing and confidentiality and security of personal data processing respectively.

this should be subject to certain exceptions outlined in the provision.[337] The Convention also prohibits the automated processing of personal data subject to certain exceptions.[338]

3.8.1.3 Rights of data subjects and duties of data controllers: Certain rights of the individuals[339] and duties of data controllers are provided for in the Convention.[340]

3.8.1.4 Exceptions: Any processing of personal data for 'public security, defence, research, criminal prosecution or state security' is exempted from the provisions of the Convention, subject to 'exceptions defined by specific provisions of other extant laws.'[341] Also exempted from the provisions of the Convention is processing carried out for personal or household activities but such data must not be for systematic communication to third parties.[342] Processing of personal data (sensitive or not) for journalistic, artistic, research and literary expression is only legitimate where it is in accordance with the codes of conduct of the profession (that is, journalistic, artistic, research and literary profession).[343]

3.8.1.5 Enforcement and supervision: Regarding enforcement, the Convention mandates state parties to establish an independent administrative authority in charge of protecting personal data which are referred to as National Protection Authorities (NPAs).[344] The duties and powers of the NPA are outlined in the Convention.[345] It is, however, observed that the Convention does not make any provision for an overall supervisory institution at the AU regional level.[346]

3.8.1.6 Transborder data flow: The Convention prohibits the transfer of personal data to non-member states of the AU except if such a state provides for an adequate level of data protection.[347] The provision is not, however, applicable where the data controller requests

337 Art 14.
338 Art 14 (5).
339 Right to information (art 16); right of access (art 17); right to object (art 18), right of rectification or erasure (art 19).
340 Duty of confidentiality (art 20); security obligations (art 21); storage obligations (art 22); sustainability obligations (art 23).
341 Art 9(d).
342 Art 9 (2)(a).
343 Art 14 (3).
344 Art 11.
345 Art 12.
346 Greenleaf & Georges (n 315 above).
347 Art 14 (6) (a).

authorisation for such transfer from the NPA.[348] The Convention does not define 'adequacy' or the criteria for determining adequacy. Greenleaf therefore argues that 'it has a meaning informed by the usage of the same term by Article 25 of the EU Directive.'[349]

3.8.2. Influence of the AU Convention on Cyber-security and Personal Data Protection on data privacy protection in Nigeria

The Convention has detailed provisions which any African country could rely on for the purpose of enacting a national legislation.[350] While the Convention is a commendable initiative, its ability to influence adequate data privacy in Nigeria appears to be limited for the following reasons. Firstly, its provisions are applicable only to state parties who have acceded to and ratified the Convention.[351] There is yet no evidence of ratification by any African state.[352] Even if it is eventually ratified by Nigeria, another limitation is that the Nigerian Constitution provides that no treaty shall have any legal effect unless it has been enacted into law by the National Assembly.[353] Thus, ratification is not enough for the Convention to be influential in Nigeria. It must also be domesticated. Unless so domesticated, no one can rely on or seek to enforce any of its provisions.[354] Domestication of the Convention by Nigeria will mean the country has bound itself to the obligations under the treaty as a consequence, it must put in place the necessary structure to ensure the fulfilment of obligations under the Convention.[355] Thus, once signed, there must be in place local laws to support compliance.[356] This is a particularly cumbersome process. Besides, if the Convention is eventually ratified and domesticated, its ability to adapt to local circumstances may limit its influence as there may be issues of compatibility. In this

348 Art 14 (6) (b).

349 Greenleaf & Georges (n 320 above). Art. 25 of the EU Directive provides for adequacy.

350 Greenleaf & Georges (n 320 above). In fact, they opine that the Convention's provisions is almost like a Model Act.

351 To be legally binding, a convention requires express consent. Parties who do not sign and ratify are not bound by its provisions. MN Shaw *International law* (2006) 89-90.

352 Details of the Convention and its status list are yet to be uploaded on the AU website. http://www.au.int/en/treaties (accessed 1 November 2015).

353 Sec 12 the Nigerian Constitution. See also the case of *General Sani Abacha v. Gani Fawahinmi* (2000)FWLR (pt. 4) 533 at 585-586 where the Nigerian Supreme Court held that '[a]n international treaty to which Nigeria is a signatory does not *ipso facto* become a law enforceable as such in Nigeria. Such a treaty would have the force of law and therefore justiciable only if the same has been enacted into law by the National Assembly...'

354 Dada (n 63 above) 41.

355 See art 8 (1) of the Convention.

356 'A report of the online debate on Africa Union Convention on Cybersecurity (AUCC)' submitted to the African Union Commission (AUC) http://www.iitpsa.org.za/wp-content/uploads/2014/02/REPORT-ON-OF-THE-ONLINE-DEBATE-ON-AFRICA-UNION-CONVENTION-ON-CYBERSECURITY.pdf (accessed 1 November 2015).

regard, Killander opines that 'the ratification of a treaty should be preceded by a compatibility study. However, such studies are not undertaken systematically in most African states.'[357] Furthermore, the Convention lacks a general body which will supervise the compliance with its provisions at the regional level.[358] It merely requires state parties to establish NPAs.[359] Another apparent omission from the Convention is a provision on co-operation amongst African states. This may limit its effectiveness in Nigeria as data privacy is now a transnational issue because of TBDF. There is, therefore, the need for an effective cooperation mechanism. The combination of cyber security, electronic transaction and data privacy in one Convention also makes it seem as if data privacy protection is only treated as an incidental matter. This is not supposed to be the case. It must, however, be pointed out that the Convention is relatively recent and it may be too early to evaluate its influence in Nigeria. All in all, the Convention is, indeed, a welcomed development to human rights in Africa.

3.8.3. Economic Community of West African States' (ECOWAS) initiatives

The ECOWAS is also mindful of the progress being made in the area of ICT and the internet which increasingly raises issues of data privacy protection.[360] It adopted the Supplementary Act A/SA.1/01/10 on Personal Data within ECOWAS 2010 ('ECOWAS Supplementary Act' or 'Supplementary Act').[361] Makulilo states that ECOWAS is the first and only sub-regional body in Africa to develop a concrete data privacy law.[362] It therefore spurred data privacy laws in West Africa.[363]

3.8.3.1 Scope: The Supplementary Act covers personal data processing by both public and private legal entities. It also applies to both manual and automated personal data

357 M Killander 'How international human rights law influences domestic law in Africa' (2013) 17 *Law, Democracy & Development* 385.

358 Unlike the EU that makes provision for Art 29 Working Parting (Art 29 WP) and the draft EU Regulation provides for a European Data protection Board (EDPB). See B Van der Sloot 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) *International Data Privacy Law* 318.

359 Art 11 (5).

360 See the ECOWAS Supplementary Act available at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf (accessed 1 November 2015).

361 The Supplementary Act was adopted at the 63rd ordinary session of the Council of Ministers held at Abuja, Nigeria from 20-21 November 2009.

362 Makulilo (n 323 above) 82.

363 G Greenleaf 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2014) 23(1) *Journal of Law, Information & Science* available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877 (accessed 1 November 2015).

processing.[364] Any personal data processing carried out in an UEMOA[365] or ECOWAS state will also be within the scope of the Supplementary Act.[366] Also within the scope of the ECOWAS Supplementary Act is data processing related to public security, defence, investigation and prosecution of criminal offences or State Security subject to the provisions of other laws in force.[367] The inclusion of data processing for public security, defence and criminal investigation within the scope of the Supplementary Act is, indeed, novel as many data privacy instruments usually exclude them from their scope *ab initio.*[368]

3.3.8.2 Principles of data processing: Basic data processing principles are contained in the Supplementary Act.[369] However, there is no special provision protecting sensitive personal data.[370] The Supplementary Act prohibits direct marketing[371] and automated processing of personal data.[372]

3.3.8.3 Rights of data subjects and duties of data controllers: The Supplementary Act provides for some rights of data subjects and obligations of data controllers.[373]

3.3.8.4 Exceptions: The Supplementary Act does not apply to data processing by an individual for the purpose of personal or domestic activities[374] and for journalistic research, artistic and literary purposes.[375]

3.3.8.5 Supervision and Enforcement: The Supplementary Act requires each member state to establish a Data Protection Authority if it does not have one.[376] The Data Protection Authority shall be an independent agency of the government.[377]

3.3.8.6 Transborder data flow: Article 36 of the Supplementary Act prohibits the transfer of personal data to non-ECOWAS countries without an adequate level of data protection.

---

364 See definition of personal data processing in art 1 of the Supplementary Act.
365 *Union économique et monétaire Ouest Africane* (UEMOA). Meaning, West African Economic and Monetary Union.
366 See art 3.
367 Art 3(4).
368 See eg, art 3(2) of the EU Directive
369 See art 23-29.
370 Art 30.
371 Art 34.
372 Art 35.
373 See chapter 6 of the Supplementary Act.
374 Art 4.
375 Art 32.
376 Art 14(1).
377 Art 14(2).

No method of assessing adequacy is stated in the Supplementary Act. Another issue with this provision is that it merely restricts transborder data flow to a non-member state without an adequate level of data protection. It does not provide for a regime regulating transfer of data between member states especial when a member state has an inadequate regime on data privacy.

3.8.4. Influence of the ECOWAS Supplementary Act on data privacy protection in Nigeria

Nigeria has an obligation to adopt a data privacy law in accordance with its obligations to ECOWAS.[378] The ECOWAS Supplementary Act is annexed to the ECOWAS Treaty which means it forms an integral part of the latter.[379] The Supplementary Act is, therefore, legally binding on the member states.[380] Thus, a violation of the Supplementary Act by a member state can be enforced before the ECOWAS Court of Justice.[381] Nevertheless, it is submitted that, given the provisions of the Constitution, the Supplementary Act cannot take effect in Nigeria if it has not been domesticated.[382] This will limit its influence in Nigeria.

The question may arise regarding the rationale for two data privacy instruments at the regional level which affects Nigeria. This question goes to the broader issue of the increasing decentralisation of data privacy policies at regional levels. A number of explanations can be given to justify this practice. Firstly, as pointed out by Kuner, '[i]n the absence of a global data protection framework, different regional standards must be able to co-exist.'[383] In essence, Kuner's statement implies that since there is no binding global data privacy instrument, attention should increasingly be turned to regional initiatives. Secondly, there is the contention that the approach to data privacy is usually a reflection of the goals and aspirations of a particular community. These aspirations are better reflected in smaller groups. Thus, it may be argued that the ECOWAS Supplementary Act is more of a reflection of the West African common aspirations on data privacy than the AU Convention. Related to the last point is the fact that because of TBDF, there is the need to

---

378 Makulilo (n 270 above) 25.
379 Art 48. See also Bygrave (n 217 above) 80.
380 Bygrave (n 217 above) 80.
381 Makulilo (n 323 above) 83.
382 See arguments in 3.8.4 above on the influence of the AU Convention in Nigeria.
383 C Kuner 'The European Union and the search for an international data protection framework' (2014) 2(1) *Groningen Journal of International Law* 69.

ensure greater harmonisation of data privacy laws. Harmonisation is, arguably, more feasible at the smaller ECOWAS level than the AU level. In conclusion, the point must be made that the Supplementary Act can only be an important addition to national efforts if the ECOWAS puts in place effective enforcement machinery and closely monitor the implementation of the Act.

3.9. Impediments to adequate data privacy protection in Nigeria

In discussing the extant legal and institutional framework on data privacy protection in Nigeria, some specific issues and challenges associated with them were analysed. This section takes the discussion further by considering the general challenges of data privacy protection in Nigeria. The issues and challenges considered in this section are of a more practical nature and constitute a summary of the reasons for the deficient legal regime in Nigeria.

3.9.1. Legal framework for data privacy protection and related issues

The first impediment to adequate protection of data privacy in Nigeria is the state of the legal framework. There is as yet no comprehensive (omnibus) law regulating data processing activities online and offline.[384] Several commentators observe that the lack of omnibus data privacy legislation is the major impediment to adequate data privacy protection.[385] Yet, it may be contended that the absence of a comprehensive data privacy legislation is not an issue *per se* because there are various laws which have the effect of protecting personal data. However, these legal instruments, as argued above, are extremely limited due to the complexities of data privacy protection. Besides, Greenleaf points out that law with respect to data privacy 'must set out data privacy principles in a specific fashion, not only as a general constitutional protection for privacy, or a civil action (tort) for infringement of privacy.'[386] These legal instruments cannot, therefore, be substituted with a comprehensive law on data privacy. That notwithstanding, it is contended that adequate protection of data privacy goes far beyond merely enacting a comprehensive legislation on data privacy.

---

384 Kusamotu (n 18 above); Obute (n 16 above) 438-439; Izuogu (n 21 above).

385 Kusamotu (n 18 above); Obute (n 16 above) 438-439; Izuogu (n 21 above). See also BO Jemilohun 'Legislating for data protection in Nigeria: Lessons from UK, Canada and India' (2010) 1 *Akungba Law Journal* 116.

386 He made this observation when identifying the criteria to access the development of data privacy legislation around the world. Greenleaf (n 363 above).

Another issue with the legal framework for data privacy protection is the multiplicity and incoherence of policies. Our analysis of the legislative efforts on data privacy protection in Nigeria illustrates this point.[387] There are numerous draft Bills which virtually have the same aims and objectives, for example, the Data Protection Bill (2010) and the Protection of Personal Information and Data Protection Bill (2012). There are also many sectoral regulations which are inconsistent. A reason for these inconsistencies in the policies on data privacy is the lack of comprehension of the rudiments of data privacy protection by policymakers. Though ICT is rapidly growing in Nigeria, the technical knowledge needed to design legislative frameworks to keep pace with these developments remains in short supply.[388] This is a major impediment to the realisation of effective data privacy protection in Nigeria.

3.9.2. Lack of commitment by the Nigerian government

The Nigerian government has simply not taken data privacy protection as a priority issue and this is another reason for the incoherence of policies on data privacy in Nigeria. This researcher has argued elsewhere that data privacy protection has not gotten the desired attention in the Nigerian jurisprudence.[389] The point was further made that there is a total neglect of issues relating to data privacy specifically and privacy in general.[390] The Nigerian government pays more attention to cybercrime than data privacy protection.[391] This is evident from the numerous laws on cybercrime and the fact that there is even a dedicated institutional framework to combat cyber criminals in Nigeria.[392] The government seems to be oblivious of the nexus between cybercrime and data privacy protection.

---

387 Discussed in section 3.7 above.

388 Gwagwa *et al* observe this in relation to Africa generally. (n 41 above).

389 Abdulrauf (n 49 above) 93.

390 Abdulrauf (n 49 above) 93.

391 There are a number of initiatives on cybercrime in Nigeria since 2004. The Nigerian National Assembly recently passed the Cybercrime Bill 2013 into law. See E Aginam 'At last, Senate passes Cyber Crime bill into law' *Vanguard newspaper* 5 November 2014 available at http://www.vanguardngr.com/2014/11/last-senate-passes-cyber-crime-bill-law/ (accessed 1 November 2015); the Nigerian Evidence Act was also amended to enable electronic documents and computer generated evidence admissible in court; the establishment of the EFCC with Economic and Financial Crime Commission (Establishment) Act 2004. See OJ Olayemi 'Combating the menace of cybercrime' (2014) 3(6) *International Journal of Computer Science and Mobile Computing* 980 – 991. For more on ICT related economic crimes and the responses of the Nigerian government, See IY Arowosaiye *Economic crimes and ICT: Response of the Nigerian criminal law* (2014).

392 The government created the Computer Crime Protection Unit (CCPU) which is under the supervision of the Public Protection Department of the Federal Ministry of Justice. The Unit works with agencies such as the EFCC, the telecommunications and banking sectors. See OJ Olayemi (n 374 above) 985. The EFCC also plays a crucial role in combating cybercrimes in Nigeria. See OJ Olayemi 'A socio-technological analysis of cybercrime and cyber security in Nigeria'6 (3) *International Journal of Sociology and Anthropology* (2014) 116-125.

Identity theft is a major means by which cyber criminals carry out their criminal activities. An effective legal framework on data privacy will go a long way in curbing identity thefts and abuse or misuse of personal data.

Similarly, laws in Nigeria generally have not kept pace with the rapid advances in technology. This is a fact which even the Nigerian Attorney General of Federation and Minister of Justice admitted.[393] Many of the existing policies, with respect to ICT are too old and are not updated. This clearly depicts the lack of commitment on the part of the Nigerian government.

Poor implementation of the available regulations and policies on data privacy also has to do with lack of commitment by the government. Existing regulations on data privacy protection are poorly implemented or do not have clear implementation strategies. There is yet no evidence that any business or government agency has been sanctioned for misuse of individuals' personal information despite a number of policies on data privacy protection in Nigeria.

3.9.3. Low level of awareness

There is very low level of awareness of the dangers of personal data processing by both the people and policymakers. A low level of awareness of privacy issues generally is not only a Nigerian problem. 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.[394] The higher the level of awareness of data privacy issues, the more likely the people will be able to demand greater protection for their personal data from the government and private entities. Moreover, the people could also play a role in data privacy protection by being more actively involved in the processing of their personal data and by asking the necessary questions from data users. Similarly, the courts can be more proactive in data privacy issues if the people institute actions for the enforcement of their right to data privacy. These can only be done with a higher level of awareness.

393 Idoko (n 371 above).

394 EM Bakibinga 'Managing electronic privacy in the telecommunications sub-sector: The Ugandan perspective' (2004) http://www.thepublicvoice.org/events/capetown04/bakibinga.doc (accessed 1 November 2015).

3.9.4. Technological backwardness and infrastructural deficits

Though Nigeria is increasingly developing technologically, there is still a high level of technological backwardness. The necessary infrastructure to facilitate access to ICT is still lacking in larger parts of the country.[395] Admittedly, technological backwardness and infrastructural deficits do not, on their own, constitute a practical challenge to realisation of the adequate protection of personal data in Nigeria. What really constitutes a challenge is the level of consciousness *vis-à-vis* the level of technological penetration in Nigeria. Scholars have over time argued that one of the reasons for the lack of awareness on the importance of data privacy is because of the technological backwardness.[396] This is because technological advances could 'influence privacy consciousness at a level that could lead to policy and regulatory responses.'[397] Thus, many people and policymakers are not conscious of threats of personal data proliferation because of the low level of exposure to technology.

Be it as it may, it is submitted that the 'digital divide'[398] in a particular society has little or no role to play in data protection as data privacy is a human right. This, by implication means everybody is entitled to such the right irrespective of where he/she resides and his/her status in the society.

3.9.5. Poor human rights track record of Nigeria

When it comes to human rights generally, the Nigerian government has a very poor track record.[399] In this regard, Akinrinade observes that:

> Even though the government sought to present a clean image on human rights, the reality was different. Abuses continued, and as the socio-economic environment deteriorated, including the

395 See 'Nigeria's National Broadband Plan 2013-2018' (n 10 above).
396 Kusamotu (n 18 above) 156.
397 Makulilo (n 323 above) 80.
398 According to Stefanick, the 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 L Stefanick *Controlling knowledge: Freedom of information and privacy protection in a networked world* (2011) 18.
399 The human rights abuses of Nigerian security agencies are one of the causes of its poor human rights records. See Human rights 'Rights abuses complicate US support for Nigeria' http://www.dw.de/rights-abuses-complicate-us-support-for-nigeria/a-17648303 (accessed 1 November 2015).

> collapse of social infrastructure, respect for human rights wore thin. The government's authoritarianism did not diminish as it held on to power.[400]

The right to data privacy will definitely be affected by this unhappy history of human rights violations in Nigeria. This is more so with the increasing security challenges and the upsurge in activities of human rights activist and opposition members. The most likely conclusion, based on Nigeria's human rights record, is that even if there are coherent policies on data privacy protection, they may not be really effectively implemented, so as to enable easy monitoring of human rights activist, opposition members and government critics.

3.9.6. Data (privacy) protection and the African culture

Culture significantly affects data privacy and may constitute a challenge to its protection in Nigeria specifically and Africa in general. A brief analysis of the difference in the values of a typical African society and a Western society will help in a proper understanding of how culture affects privacy and data privacy Nigeria. A typical Western society is deeply individualistic in nature and promotes the concept of individualism as a fundamental concept of law and justice.[401] Thus, Western culture focuses more on how to promote a person as an individual within the society and upholds his right to private life.[402] An individual in a Western society is given the autonomy to develop himself privately without any form of interference from both his community and the government.[403] Western societies are therefore deeply rooted in respect for the privacy and the personal autonomy of an individual as a means of effective realisation of their right to self-development.

The concept of individualism is alien to indigenous communities in Africa. It should be said, though, that it is impracticable to view Nigeria and Africa as a single homogenous society as they are deeply socially and culturally fragmented.[404] Indigenous Nigerian

---

400 B Akinrinade 'Human rights NGOs in Nigeria: Emergence, governmental reaction and the future' (2002) 2 *African Human Rights Law Journal* 125; See also Frontline Protection of Human rights defenders 'Nigeria: Defending human rights: Not everywhere not every right international fact finding mission' April 2010 available at http://www.omct.org/files/2010/05/20688/nigeria_mission_report.pdf (accessed 1 November 2015) 6.

401 MM Akanbi *Domestic commercial arbitration in Nigeria: Problems and challenges* (2012) 12. See also Allotey (n 65 above) 152-153.

402 Allotey (n 65 above) 151.

403 Makulilo (n 323 above) 78.

404 A commentator explains that 'again, one cannot speak and write about Africa as if it were a single, homogeneous society, or even a series of isolated, ethnic groups, all basically similar or comparable. On the contrary, Africa is (and was) socially and culturally very fragmented indeed.' Nevertheless, he

societies are bound as a group which brings about a communal relationship. The interest of the group or community far outweighs that of a single individual.[405] The collective interest is paramount and individualism is submerged.[406] The individual's identity is derived from the group identity and the group's identity is visible in the interactions between groups, families, communities, clans, villages, chiefdoms etc.[407] Anyone who places himself outside the life and normal working of the group constitutes a threat to the working of the whole group.[408] The concept of communalism applies in the Muslim community which also forms a predominant section of the Nigerian society.[409] Therefore, a typical African society is characterised by openness and interdependence.[410]

The African philosophy of communalism has implications on data privacy because of its relationship with privacy. Thus, it is arguable that because of the communal lifestyle in Nigeria, the right to data privacy will be suppressed. The intersection between data privacy and culture will therefore appear to be a challenge. Nevertheless, it must be pointed out that the traditional Nigerian society is fast giving way to a modern Nigeria. Hence, communal Nigeria is gradually becoming individualistic as a result of globalisation and westernisation of culture.[411] People are gradually beginning to appreciate the importance of privacy related issues. Yet, the existence of privacy and the 'push' by the West for countries to adopt privacy and data protection standards have been criticised by some scholars as being 'cultural imperialism.'[412] Hence, cultural arguments have more often been used against the adoption of privacy rules.[413] Makulilo, however, points out that though the community comes first in African culture, 'privacy will still be an important

---

notes that in spite of this discouraging pluralism 'it is possible to discern certain regularities' A Shorter 'Concepts of social justice in traditional Africa' http://www.afrikaworld.net/afrel/atr-socjustice.htm (accessed 1 November 2015).

405 It has been opined that 'there are arguments, but rarely supported by empirical evidence, that in Africa group interests outweigh individual interests due to the culture of collectivism; hence claims for privacy are less common.' Makulilo (n 323 above)78.

406 A Allot 'African Law' in JDM Derrett (ed) *An introduction to legal systems* (1968) 131.

407 Shorter (n 399 above). Akanbi (n 400 above) 120.

408 Shorter (n 399 above). Akanbi (n 400 above) 120.

409 Islam encourages brotherhood. It is one of the basic principles of the Sharia that the interest of the society takes precedence over the interest of the individual. See generally A Doi *Sharia: The Islamic Law* (1990) 11.

410 Allotey (n 65 above) 154.

411 For more on westernisation of culture in Africa generally and Nigeria in particular, See D Arowolo 'The effects of western civilization and culture on Africa' 1(1) *Afro Asian Journal of Social Sciences* (2010).

412 Makulilo (n 323 above) 78.

413 Makulilo (n 323 above) 78.

concern as the information technology revolution advances.'[414] Besides, some scholars have tried to dissociate data privacy form the 'individualistic features' of privacy, as it is arguable that, data privacy merely sets out rules on the lawful processing of information that is considered personal.[415]

3.9.7. Security challenge

While many African states seek to consolidate democratic gains and are working towards peace and stability in the continent, they are facing new threats posed by cybercrime and terrorism.[416] In Nigeria particularly, the security challenges are enormous and make the government use every means at its disposal to curb insecurity. The government has increased its surveillance activities both online and offline. Many policies are put in place to facilitate easy identification of citizens such as SIM card registration, BVN and other schemes. These initiatives, as previously argued, are obstacles to the adequate protection of data privacy in Nigeria.

The practical manifestation of insecurity issue as an impediment to the adequate protection of data privacy in Nigeria is that the government is usually very suspicious of any policy which has to do with enhancing individuals' right to data privacy and access to information. The suspicion is better reflected in the reluctance of the government to adopt the FOIA.[417] In the same light, many laws grant the government significant exemptions (without concrete reasons) to allow access to personal data of individuals. This is not totally unconnected with the long period of military dictatorship in Nigeria.[418]

3.10. Chapter conclusion

This chapter set out to investigate why data privacy should be protected and how it is protected in Nigeria. For this purpose, the chapter analysed the overall legal framework for data privacy protection in Nigeria and interesting findings were made. Before that, however, the chapter reflected on current issues on data privacy in Nigeria. It considered

414 Makulilo (n 323 above)79

415 See eg, S Rodotà 'Data protection as a Fundamental right' in S Gutwirth *et al* (eds) *Reinventing data protection* (2009) 79-80.

416 Gwagwa (n 41 above).

417 The FOIA took years in the National Assembly before it was finally enacted as law. See (n 306 above).

418 Many laws in Nigeria were passed as Decrees during the Military era and they have not been substantially amended or modified. Even as Nigeria has returned to civilian rule, some of the leaders are ex-military officers. Eg, the former President Olusegun Obasanjo and the President of Nigeria's Senate, Senator David Mark, who were both high-ranking military officers.

contemporary data processing activities in Nigeria by both public and private data controllers. The argument was made that, contrary to the contention of some scholars, there is an increasing level of processing activities in Nigeria. The section of the chapter concluded that there is the presence of 'big data' and 'big brother' phenomenon in Nigeria because of the large number of databases and surveillance activities.

The observation that there is an increase in databases and surveillance activities led to an examination of the legal regime of data privacy protection in Nigeria. The protection of personal data under the Nigerian Constitution, the ACHPR and the common law was investigated. With regard to the Constitution, it was found that section 37 has an extremely limited scope as it protects the privacy of Nigerians only. The ACHPR on the other hand has no provision on the right to privacy; however, wider interpretation of some of its provisions may provide limited protection for data privacy. In the same light, the common law in Nigeria was found to be very limited in its protection of data privacy. On the whole, the chapter observed that the Constitution, ACHPR and the Common law are only limited to realising a part of the essence of data privacy law, which is the protection of the confidentiality of private information. Access to personal data which is the other essence of data privacy law is not covered by these laws.

The chapter therefore went further to examine the protection of data privacy in other laws (sectoral laws). Three laws were identified which have provisions relating to data privacy protection, that is the FOIA, the National Health Act and the Statistics Act. The provisions on data privacy were analysed. Two important findings were made regarding the other legislative protection of data privacy in Nigeria. First, many sectors that carry out significant processing of personal data do not have data privacy provisions in their laws. Second, recent sectoral laws do not contain elaborate provisions on data privacy protection in line with international practice.

An analysis was carried out of institutions relevant for personal data protection in Nigeria. The NCC, NITDA, NIMC and the courts were discussed. It was observed that the main legislation establishing these government agencies and empowering them (in some cases) to carry out processing of personal data, do not contain data privacy provisions. However, these institutions, in many instances, have non-binding legal instruments regulating data processing activities. The point was also made that non-binding instruments are not as effective as legislation. With respect to the courts, it was noted that they have not been

proactive in their functions as custodians of human rights relating to privacy generally. The crucial finding of this section of the chapter was that there are legal instruments which make provision for data privacy protection that many people are oblivious of.

In order to advance the literature on data privacy protection in Nigeria, the chapter reviewed the legislative efforts towards data privacy protection in Nigeria. It reiterated the fact that there are several Bills before the National Assembly which have the effect of data privacy protection; however, two are noteworthy. They are the Data Protection Bill 2010 and the Personal Information and Data Protection Bill 2012. Several lacunae were identified in the Bills which may limit their ability to influence adequate data privacy protection. The findings of this chapter regarding the Bills are that: First, the Nigerian legislature is not committed to passing the Bills into law. Second, policymakers who draft the Bills do not have an in-depth knowledge of the law on data privacy. The draft Bills' ability to adequately protect personal data may therefore be limited if any of them is eventually enacted into law.

The forgoing analysis in the chapter showed that the current legal framework on data privacy is inadequate to protect the data privacy of Nigerians. Unfortunately, the draft Bills may also suffer a similar fate. Attention was therefore turned to regional and sub-regional initiatives towards data privacy protection. It was observed that in the absence of ratification and domestication by the Nigerian government, these instruments cannot influence the adequate protection of data privacy of individuals in Nigeria. Moreover, commitment by the government to implement these instruments is paramount to achieving their objectives.

In summary, the most important observations of the chapter regarding data privacy protection in Nigeria are: first, the development of ICT is not followed with a corresponding improvement in the legal framework that addresses the challenges of personal data processing. Second, there is an absence of a quality legal framework on data privacy protection and weak enforcement of available regulations. Third, the people are either not aware of their rights, or in some cases, there is a sheer nonchalant attitude towards the use of their personal information.

A commentator rightly observes that 'data protection is a huge deal because you are your data.'[419] An individual's personal data is therefore an embodiment of his/her personality. It processing without effective regulations threatens the very essence of his/her being. Urgent steps must therefore be taken before 'it is too late to put this technological genie back in the bottle.'[420] Consequently, the next chapters will examine other jurisdictions for solutions to this problem.

419 Comment made in Oguntimehin (n 23 above).

420 Lloyd uses the term 'technological genie' to refer to 'potentials for misuse' of personal data. Thus if society do not quickly realise the potentials for misuse of personal data, it may be too late to reverse this trend of abuse of personal data. Lloyd (n 1 above) 25.

Chapter four

An analysis of the legal framework for the protection of data privacy in Canada: Lessons for Nigeria

4.1. Introduction

> *With reference to the formation of Canadian [data] privacy policy… it is demonstrated that the lessons drawn from the experience of other countries' legislative attempts to protect personal data were instrumental in shaping a Canadian policy. Lessons about the principles of data protection, the exemptions to those principles, and the policy instrument to implement them were drawn at critical stages from American, and other experience. The fact that some lessons were drawn and not others, from some countries and not others, helps us understand why Canadian privacy policy is as it is today.*[1]

The quotation above provides a useful entry point into the subject of this chapter and it highlights two vital points with respect to a proposed data privacy framework in Nigeria. The first is the essence of lesson-drawing for the purpose of legal and policy formulation on data privacy.[2] In this respect, for Nigeria to develop an effective framework for data privacy, lessons must be drawn from the experiences of other countries. The second point is the importance of selectivity in lessons-drawing. The point is clear from Bennett's statement that 'the fact that some lessons were drawn and not others' and 'from some countries and not others' shows that not every feature of a particular legal system is relevant for another. With respect to data privacy, not every country's experience can be workable in Nigeria. A feature of a data privacy regime of another country, may only be borrowed if it is likely to aid effective data privacy protection in the Nigerian context.

---

1 CJ Bennett 'The formation of a Canadian privacy policy: the art and craft of lesson-drawing' (1990) 33 *Canadian Public Administration* 553.

2 Bennett (n 1 above) 553.

In the light of the above, this chapter analyses the legal regime of data privacy protection in Canada. This is with a view to identifying possible lessons that can be drawn from the Canadian experience. For vital lessons to be obtained, analysis of the Canadian data privacy framework will be carried out based on the Article 29 Working Party (WP) methodology.[3] The European Commission (through Article 29 WP) is the only institution that has developed a coherent methodology for assessing 'adequacy' of legal regimes for data privacy protection although, with respect to transborder data transfers.[4] Even though this standard has over time been criticised,[5] it seems to be generally accepted worldwide as an effective standard as many countries strive to obtain an adequacy finding from the EU.[6] The adequacy standard developed by Article 29 WP is contained in two documents: the WP 4[7] and WP 12.[8] WP 12 is, however, currently regarded by the EU as authoritative.[9] WP 12 sets two levels of assessment of adequacy, the first is the content principle and the second is the procedural/enforcement principle. The content principle is largely based on the contents of data privacy legislation with particular focus on the strengths of the fair information principles (FIPs). The procedural requirements, for the most part, focus on the enforcement and implementation mechanism of a data privacy law.

---

3 Art 25 of the EU Directive provides that transfer of personal data to 3rd countries from an EU member state can only be carried out if the 3rd country has an 'adequate level' of protection for personal data. Art 25 (6) empowers the EU Commission to make general determination of adequacy. In practice, such decision is usually arrived at with a non-binding opinion from a WP established by art. 29 of the EU Directive, usually called Article 29 WP ('Art 29 WP').

4 Though there are several criticisms against the EU data protection regime especially because of its 'adequacy requirement'. The 'one size fits all' approach adopted by the EU Directive and most especially, the draft EU Regulation has been severely criticised. In fact, some scholars have even recommended that we go back to the strict OECD Guidelines regime which is an approach largely adopted by the Canadian regime. See B Koops 'The trouble with European data protection law' (2014) 4 *International Data Privacy Law* 250-261.

5 Criticisms are mainly as a result of the fact that the criteria of Art 29 WP are largely towards ensuring that Europeans' personal data being transported to other countries for processing are properly protected. It does not take into consideration the personal data of individuals in the host or receiving country. See MD Birnhack 'The EU Data Protection Directive: An engine of a global regime' (2008) 24(6) *Computer Law & Security Report* 513. He contended that '[t]he declared goal is framed in a rather modest self-interest spirit: adequacy of third countries is important so [sic] to protect the interests of European data subjects.' See also AB Makulilo 'Data protection regimes in Africa: Too far from the European 'adequacy' standard?' (2013) 3 *International Data Privacy Law* 50.

6 Including many African countries such as Burkina Faso, Tunisia, Morocco and Mauritius. See generally Makulilo (n 5 above) 42-50.

7 Art 29 Data Protection Working Party 'Discussion document: First orientations on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy' XV D/5020/97-EN final WP4 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf (accessed 1 November 2015).

8 Art 29 Data Protection Working Party 'Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive' DG XV D/5025/98 WP 12 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf (accessed 31 November 2015).

9 Makulilo (n 5 above) 44.

The chapter will therefore scrutinise the statutory and institutional framework for data privacy in Canada. The contents of the major laws and the oversight and enforcement mechanism will be analysed so as to expose vital lessons for Nigeria. The interaction between the Canadian and international data privacy framework will also be considered to see if there are any influences in enhancing data privacy protection in Canada. This chapter also examines the EU Commission's adequacy finding on the Canadian data privacy framework. Furthermore, some consideration is given to the on-going legal reforms of the Canadian framework which may provide useful lessons for any jurisdiction. The chapter concludes by highlighting vital insights a country like Nigeria can gain from Canada for developing a framework on data privacy.

For the purpose of clarity, the discussion in this chapter is limited in two ways. First, the chapter focuses on only the legal framework[10] for data privacy at the federal level as it is practically impossible to consider all Canadian legal and policy frameworks within the scope of this chapter.[11] Hence, only a distinguishing feature of a provincial data privacy law which is substantially different from the federal law shall be highlighted.[12] Similarly, the chapter analyses only laws that protect personal data as narrowly construed and not the general laws on privacy.[13] Second, though the chapter seeks to draw lessons for Nigeria, the applicability or suitability of lessons drawn will not form part of the discussion herein.

---

10 In this case, legislation *strico sensu* because of the trend of protecting personal data via legislation only. Stefanick opines that '[m]ost [data] privacy protection comes by virtue of laws passed in legislatures that seek to give individuals control over their persons. In the last few decades, countries around the world have developed information privacy legislation that seeks to protect the privacy of information held by governments.' L Stefanick *Controlling knowledge: Freedom of information and privacy protection in a networked world* (2011) 38. See also CJ Bennett & CD Raab *The governance of privacy* (2006) 125-126.

11 It is also practically impossible within the scope of this chapter to discuss all provincial statutes on data privacy. Moreover, 'while there are a number of important differences in both content and wording between the various privacy statutes, all cover the same essential principles and obligations.' D Elder 'Canada' in M Kuschewsky (ed) *Data protection and privacy: Jurisdictional comparisons* (2012) 42.

12 Except for the health sector as will be shortly seen. This specifically dedicated health sector laws are available only in the provinces.

13 As a consequence, legislation such as the Canadian Criminal Code and laws of tort will not be considered. It is very important to draw this fine distinction between laws on privacy generally and data privacy laws. This is especially so when considering the legal framework on personal data protection in jurisdictions such as Canada, the US, New Zealand and Australia. These regimes do not make a water-tight distinction between the rules on privacy and data protection unlike the Europeans. Such may bring about confusion and unnecessarily broaden the scope of the discussion. It must also be stated that even though some sectoral laws have provisions protecting personal information, I will not be considering those laws as the presence of other privacy rated legislation do not mean that the federal privacy laws will not apply.

The chapter only highlights the lessons and contextualises them for application in subsequent chapters. [14]

4.2. The nature and challenge of data processing in Canada: Any similarity with Nigeria?

Several authors have written on a wide range of data privacy issues in Canada. Unlike Nigeria, Canada can be classified as an advanced nation which makes issues of processing of personal data and challenges of data privacy more advanced and complex. Yet, at some basic level, certain data privacy issues are similar to what obtains in Nigeria. The challenges identified by commentators are largely consistent with the global demand for personal information. The first category of data privacy challenges in Canada arises from the private sector, as a result of the need for personal data for commercial purposes. Piper observes that the primary collectors of personal information in the Canadian private sector are banking institutions, insurance and credit card companies, private sector health care providers, telecommunications and cable companies, chartered accountants and business involved in direct marketing.[15] Several privacy intrusive means are used for these collections without, in many cases, the knowledge and consent of the individuals. Still in the private sector, personal information is being collected and used for security purposes, sometimes in violation of data privacy right. Video surveillance constitutes a major area of concern in this category. Bennett and Bayley opine that:

> As in other industrialized states, video surveillance technologies[16] have crept into Canadian life. Cameras have been common occurrences in high-risk private spaces such as banks, in workplace, late-night or retail outlets where theft is prevalent, in transportation hubs and in shopping malls.[17]

---

14 Applicability of lessons expounded will be considered more elaborately in chapters 6 and 7 of this thesis.

15 T Piper 'The Personal Information Protection and Electronic Documents Act: A lost opportunity to democratize Canada's "technological society"' (2000) 23 *Dalhousie Law Journal* 256, she cited information obtained from an array of sources, see footnote 8 of the article.

16 As admitted by Bennett and Bayley, video surveillance technology is a rather nuanced concept and difficult to define. Traditionally, it was understood to mean CCTV cameras but with the ubiquity of these devices, it becomes difficult to define. Cameras are now 'miniaturized, and have converged with other technologies. The can pan and zoom, provide high definition images digitally to a number of destinations.' CJ Bennett & RM Bayley 'Video surveillance and privacy protection law in Canada' in S Nouwt *et al* (eds) *Reasonable expectations of privacy?* (2005) 61-62.

17 Bennett & Bayley (n 16 above) 61. Though the authors rightly admitted that '[t]he streets of Canadian cities… are not monitored to anything like the extent as in other countries, such as United Kingdom.' Recent research also shows that work place surveillance is on the increase in Canada. See A Levin 'Big and little brother: the potential erosion of workplace privacy in Canada' (2007) 22 *Canadian Journal of Law and Society* 197-230.

Like Nigeria, data processing for law enforcement and security purposes is a major cause of concern in Canada's public sector. Bennett and Bayley consider issues with the use of video surveillance for law enforcement purposes in Canada.[18] Yusuff carries out a similar study with focus on the challenges of the use of security (CCTV) cameras for law enforcement purposes which has proliferated in the country.[19] Similarly, Piper discusses other uses of personal data in the public sector such as for censuses, custom declaration, information provided for tax and election purposes.[20] Advances in technology further blur the line between private and public sector data collection practices which is another dimension to the threats to data privacy in Canada. One of the implications of this (private and public sector collaboration), as identified by Bailey, is the 'systematic government access to private-sector data in Canada'.[21] The gradual increase in the use of unique identifiers has further facilitated the cross-sector access to individual personal data.[22]

The US, appears to pose the greatest challenge to data privacy in Canada. Apparently, the 'might' of the US has forced certain data processing practices which threaten individuals' right to data privacy.[23] Challenge to data privacy brought about by the US can be seen in both sectors in Canada. In the private sector, the greatest threat to data privacy is brought about as a result of outsourcing activities between Canadian and US businesses or US businesses with affiliates in Canada.[24] Geist and Homsi, for example, reported concerns over the risks associated with outsourcing British Columbia's Medical Services Plan to

---

18 Bennett & Bayley (n 16 above) 61-62.

19 AOA Yusuff 'Legal issues and challenges in the use of security (CCTV) cameras in public places: Lessons from Canada' (2011) 23 *Sri Lanka Journal of International Law* 33-76. For more analysis on video surveillance in Canada see K Walby 'Little England? The rise of open-street closed-circuit television surveillance in Canada' (2006) 4 *Surveillance & Society* 29-51.

20 Piper (n 15 above) 256.

21 J Bailey 'Systematic government access to private-sector data in Canada' (2012) 2 *International Data Privacy Law* 207-219.

22 Eg, social insurance numbers (SIN). For more on SIN as a threat to privacy in Canada. See DH Flaherty & Canada Department of Justice *The origins and development of social insurance numbers in Canada* (1981).

23 The Former Canadian Privacy Commissioner seems to share a similar view. In one of her addresses, she pointed out that '[w]hat happens in the United States can have substantial consequences for Canada. All Canadians are aware. We are a geographically large country, but with a population that is a small fraction of that of the United States. We are therefore not as economically powerful, and we are strongly affected by the actions and attitudes of the US.' J Stoddart 'Data protection and security: A transnational discussion' an address on May 5, 2006 available at https://www.priv.gc.ca/media/sp-d/2006/sp-d_060505_e.asp (accessed 1 November 2015).

24 In a report titled 'Privacy and computers: A report of a task force' in 1972, the fact was clearly highlighted that Canadian record keeping organisations shared personal data of Canadians with US institutions like credit bureaus, insurance companies etc. See SL Mhlaba 'The efficacy of international regulation of transborder data flows: The case for clipper chip' (1995) 12 *Government Information Quarterly* 354.

US-based multinational corporations.[25] These outsourcing deals will naturally involve mass movement of personal data between the countries. Bennett *et al* also observe that many US companies with or without corporate headquarters in Canada, rarely comply with Canadian data privacy laws.[26] Of far greater concern is the influence of US on Canadian public sector data processing practices for national security purposes. In this regard, Jennifer Stoddard, the former Canadian Privacy Commissioner, observes that:

> [t]he preoccupation of the United States about national security in particular has had consequences for Canada. As allies, we have of course long shared information among our police and intelligence agencies. That sharing is on the increase, and means that ever-greater amounts of personal information about Canadians will end up in the hands of US government agencies.[27]

The threats the US poses to Canada on the grounds of national security came to a peak after the 9/11 attack, which has made the US to put more pressure on its neighbours to collect personal data and make this available to their security agencies.[28] This is particularly conspicuous in the Canadian aviation sector where airlines are required to make available personal data of Canadians entering or coming out of the US.[29] Bennett and French consider the practical implication of this on Canada, especially with respect to law enforcement, international travels and internet surveillance.[30] Data privacy concerns

---

25 M Geist & M Homsi 'Outsourcing our privacy?: Privacy and security in a borderless commercial world (2005) 554 *University of New Brunswick Law Journal* 276. See also L Stefanick 'Outsourcing and transborder data flows: The challenge of protecting personal information under the shadow of the USA Patriot Act' (2007) 73 *International Review of Administrative Sciences* 531-548.

26 CJ Bennett *et al* 'Forgetting, non-forgetting and quasi-forgetting in social networking: Canadian Policy and corporate practice' in S. Gutwirth *et al* (eds) *Reloading data protection* (2014) 47.

27 Stoddard (n 23 above).

28 This is largely due to the requirements of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT) which grants extensive powers to US security agencies to carry out privacy intrusive surveillance practices for the purposes of preventing terrorism which privacy advocates have severely criticised. This is obvious from the title of the law which is 'An Act to deter and punish terrorist acts in the United States and *around the world*, to enhance law enforcement investigatory tools, and for other purposes.' The law amended the provisions of several privacy protecting statutes in the US and weakens data privacy in the US. The law is available at http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf .Several authors have written on the effects of this law on foreign data processing practices. See eg, PT Jaeger *et al* 'The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act' (2003) 20 *Government Information Quarterly* 295-314.

29 CJ Bennett 'What happens when you book an airline ticket? The collection and processing of passenger data post-9/11' in E Zureik & MB Salter (eds) *Global surveillance and policing: Borders, security, identity* (2005) 113-138. Unlike the EU, Canadian airlines and transport authorities have consistently and willingly submitted to requests of the US for passenger information. See J McClennan & V Schick '"O, privacy" Canada's importance in the development of the international data privacy regime' (2007) 38 *Georgetown Journal of International Law* 674,675.

30 C Bennett & M French 'The State of privacy in the Canadian State: Fallout from 9/11' (2003) 11 *Journal of Contingencies and Crisis Management* 2-11. See also AJ Cockfield 'The state of privacy

influenced by the US are further intensified by the generally acknowledged weak legal regime on data privacy in the US.[31]

All the above raise a number of human rights questions such as the purpose of collection and use of personal information, accuracy and security of personal information and most of all, if such information is collected fairly and lawfully (with knowledge and consent). The Canadian legal system has indeed responded to some of these legal issues which may show an insight for Nigeria. Before considering these responses, it is important to discuss more on the reasons for the choice of Canada as a model for this study which is not totally unconnected with the country's conceptual basis and approach to data privacy protection.

4.3. The conceptual basis and approach to data privacy protection in Canada

Canada, like Nigeria, operates a federal system of government where power is shared between the central government and the provinces/territories.[32] The Constitution of Canada provides for the powers of the federal government and the provinces and the Charter contains fundamental rights provisions applicable against all levels of government.[33] Canada is also a parliamentary democracy founded on the rule of law.[34] Like Nigeria, the country is a multi-cultural society.[35] However, two major facts distinguish both countries which may have some impact on this study. First, the level of technological development is much higher in Canada leading to more complex data privacy issues. Related to this is that there is more awareness on data privacy issues because of the sophisticated nature of the Canadian society. Nevertheless, it is submitted that these issues may not be a limitation

laws and privacy encroaching technologies after September 11: A two-year report card on the Canadian government' (2003-2004) 1 *University of Ottawa Law and Technology Journal* 325.

31 Especially for the private sector. See R Moshell '…and then there was one: The outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection' (2004-2005) 37 *Texas Tech Law Review* 357-432.

32 K Klein *Canadian privacy: Data protection law and policy for the practitioner* (2012) 7.

33 Bailey (n 21 above) 207; Bennett & Bayley (n 23 above) 62; just like Nigeria where the Constitution has similar provisions in secs 33-46. See Constitution of the Federal Republic of Nigeria (1999).

34 Bailey (n 21 above) 207.

35 See A Levin & M J Nicholson 'Privacy law in the United States, the EU and Canada: Allure of the middle ground' (2005) 2 *University of Ottawa Law & Technology Journal* 393. The previous chapter (chapter 3) has considered the impact of culture on privacy and data privacy protection. It was argued that what one society or culture considers as private information may not necessarily be so considered in another society or culture. This, in my view, affects the regulation of personal data processing in several ways. Eg, an individual in a particular community may consider information such as his/her sexual life as personal information and should be protected by data privacy law. However, this may not be so for an individual in another society. Thus, Stefanick points out that '[n]otions of what properly comprises an individual's "personal" space are both culturally derived and evolving along social norms.' (n 10 above) 60.

per se as the level of technological development in Nigeria is growing and with this, awareness level will also gradually improve.[36]

Generally, Canada has been substantially influenced by its closest neighbour to the south, the US, in regulating the collection and use of personal data.[37] Thus, the law protecting Canadians' personal information is called the law of 'privacy' (the same way it is being referred to in the US) as against 'data protection' or 'data privacy' as it is generally known in Europe.[38] Nevertheless, the Canadian regime has also immensely drawn from the EU's approach especially in regulating private sector data processing activities and supervisory agency. This is why authors generally contend that the Canadian jurisprudence on data privacy shows substantial influence from both the EU and the US.[39] Hence, McWilliam posits that '[t]he regulation of privacy in Canada falls between the 'hands-off' approach in the United States and the more protective approach in Europe.'[40] In other words, Canada's approach is unique in that it tries to maintain a difficult balance between the EU strict protectionist approach and the American *laissez-faire* approach.[41] The *middle ground* is the common term used to describe the Canadian position as the EU and the US approaches are generally viewed to be at opposite ends of the spectrum.[42] The middle ground approach is also visible in the regulatory model adopted by Canada. Unlike the EU (with a comprehensive regulatory model) and the US (with a self-regulatory model), Canada's approach is a *co-regulatory model* 'where the data collection industries develop the

---

36 It may be said to be improving because of the number of academic writings exposing data privacy issues.

37 Bennett (n 1 above) 533.

38 See M Zalnieriute 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) 0 *International Journal of Law and Information Technology* 105. LA Bygrave *Data privacy law: An international perspective* (2014) 23. Though some Canadian writers acknowledge the differences between both terms. Bennett for example points out that '[a] conceptual distinction should first be made between privacy and data protection. The latter is probably a more precise appellation for policies directed towards the protection of personal information.' Bennett (n 1 above) 555. Other North American commentators try to circumvent the apparent confusion associated with the use of both terms by simply using 'information privacy'. See eg, DE Newman 'European Union and United States personal information privacy and human rights philosophy- is there a match?' (2008) 22 *Temple International and Comparative Law Journal* 307-343.

39 Bennett contends that '[i]t will be wrong to conclude that Canada emulated any one country, because the consensus was widespread' Bennett (n 1 above) 563.

40 B McWilliam 'Canada' in D Campbell (ed) *The Internet: Laws and regulatory regimes* (2013) CDN 10. Similarly Jennifer Stoddart opined that Canadian data privacy regime 'is a tailored blend of European and American data protection principles which has grown over 25 years through Supreme Court of Canada interpretations and the realities of ever-changing business imperatives.' Stoddart (n 23 above).

41 McClennan & Schick (n 29 above) 671.

42 See generally Levin and Nicholson (n 42 above); TD Nova 'The future face of the worldwide data privacy push as a factor affecting Wisconsin business dealing with consumer data' (2004) 22(3) *Wisconsin International Law Journal* 771.

privacy protection rules and those rules are enforced by industry and overseen by a privacy agency.'[43] This, it is submitted, presents a unique structure for the purpose of lesson-drawing.[44]

The conceptual underpinning of data privacy in Canada is, arguably, at variance with what obtains in both US and EU. Levin and Nicholson contend that the conceptual basis plays a significant role in the distinct approaches to (data) privacy in each of these jurisdictions.[45] The commentators maintain that the conceptual basis for (data) privacy in Canada is a middle ground between the EU and the US.[46] In the US, (data) privacy is perceived as essential for protection against government intrusion into private lives. Thus, Americans are more worried about the state's processing of their personal data rather than private entities which is why there are considerable laws regulating the government's data processing activities. Hence, data privacy protection is basically for the purpose of protecting Americans' right to liberty against the state.[47] When other laws attempt to regulate data processing in the private sector, an alternative justification for such a regulation is sought.[48] On the other hand, the conceptual basis for data privacy in the EU is that of protection of dignity. According to Levin and Nicholson, '[d]ignity protection is conceptually distinct from liberty protection. "Liberty" is a political value. "Dignity" is a social concept. To protect dignity is to protect a certain status, a certain image of one that society holds.'[49] In essence, while 'liberty is at the basis of an individual's relationship with government, dignity is at the basis of an individual's relationship with other members of the society.'[50] Dignity as a conceptual basis in the EU is not surprising as the EU Constitution states that the EU is founded on the value of human dignity.[51]

---

43 Craig & Ludloff (n 11 above) 27; see also discussions on a co-regulatory model in chapter 2 (2.8) of this thesis.

44 I will discuss the reasons why in subsequent chapters.

45 Levin & Nicholson (n 35 above) 357, 360.

46 Levin & Nicholson (n 35 above) 357, 360.

47 Levin & Nicholson (n 35 above) 382-388. The authors contend that '[f]rom our examination of the US privacy legislation and the legislation that indirectly addresses privacy concerns, it seems to us that privacy is on the whole taken to protect liberty more than dignity. The *Privacy Act, Privacy Protection Act, Driver's Privacy Protection Act, Right to Financial Privacy Act, ECPA, and FERPA, are all concerned with protection of personal information from falling into the hands of the government, or if already in the hands of government, from abuse.'* 386. (Emphasis added).

48 Levin & Nicholson (n 35 above) 387. This is because privacy is only meant to protect liberty. Liberty is construed in terms of protection against the government alone not private entities.

49 Levin & Nicholson (n 35 above) 388-389.

50 Levin & Nicholson (n 35 above) 391.

51 See the 2nd paragraph of the Charter of the Fundamental Rights of the European Union which states that 'the Union is founded on the indivisible, universal values of human dignity, freedom, equality and

While (data) privacy is for the protection of liberty of the Americans and dignity of the Europeans, Levin and Nicholson argue that a middle ground can be found.[52] Thus, both concepts may seem distinct, yet they can be understood both as manifestations of autonomy.[53] Autonomy is therefore the middle ground, which is the conceptual basis for (data) privacy in Canada.[54] Canadians therefore seem to be concerned about their data privacy, not only because it infringes their liberty when misused by the government or violates their dignity when mishandled by the private sector, but because they 'do not want to lose their autonomy, their control over this information, which is, after all, personal.'[55] Thus, the Standing Committee on Human Rights and the Status of Persons with Disabilities noted with respect to the conceptual basis of privacy that '[t]o the ordinary Canadian, it is about control - the right to control one's personal information and the right to choose to remain anonymous. Privacy is a core human value that goes to the very heart of preserving human dignity and autonomy.'[56]

Nigerians, like Canadians, ought to be worried about both private and public sector collection of personal information.[57] Thus, the conceptual basis of data privacy may be argued to be that of protection of autonomy. This makes Canada an important case study for this research. Further effects of autonomy and control as a conceptual basis of data privacy in Canada can be seen in its legal framework which will now be discussed.

---

solidarity…' The whole of chapter one of the Charter is devoted to dignity. See Charter of Fundamental Rights of the European Union (2000/C 364/01) available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 1 November 2015). See also Levin & Nicholson (n 35 above) 391.

52 Levin & Nicholson (n 35 above) 391, though they cautioned that this should not be watertight as Americans may perceive privacy as enhancing dignity and European may view privacy as enhancing liberty.

53 Levin & Nicholson (n 35 above) 391.

54 Levin & Nicholson (n 35 above) 392.

55 Levin & Nicholson (n 35 above) 392.

56 House of Commons Standing Committee on Human rights and the Status of Persons with disabilities 'Privacy rights and new technologies: Consultation package' in *Privacy: Where Do We Draw the Line?* Appendix i, 1 available at https://www.priv.gc.ca/information/02_06_03d_e.pdf (accessed 1 November 2015).

57 Issues of private and public collection of personal data have been analysed in chapter 3 (3.3) of this thesis.

4.4. The legal framework for data privacy in Canada

4.4.1. Constitutional protection of data privacy

The Canadian Charter of Rights and Freedoms [58] ('Canadian Charter') is the highest legal authority for the protection of data privacy domestically.[59] Paradoxically, it does not contain any provision on the right to privacy let alone data privacy.[60] Nevertheless, certain provisions could be interpreted as protecting dignity, autonomy and privacy which are all part of the basic interests data privacy seeks to protect.[61] With regard to privacy particularly, sections 7 and 8 are the most notable provisions used to impute its applicability.[62] Section 7 provides that '[e]veryone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.' Similarly, section 8 stipulates that '[e]veryone has the right to be secure against unreasonable search or seizure.' The requirement in section 8 was engaged in *Hunter v Southam, Inc*,[63] as it relates to what constitutes 'unreasonable' in that context. Dickson J admitted that the term is 'vague and open' as '[t]here is no specificity in the section beyond the bare guarantee of freedom from "unreasonable" search and seizure.'[64] Using a purposive approach to analyse the provision, he observed that the guarantee to be 'secure from unreasonable search and seizure' which is expressed in a negative form, is capable of a positive connotation as a protection of 'reasonable expectation of privacy.'[65] In essence therefore, it is clear from this seminal decision that

---

58 Canadian Charter of Rights and Freedoms ('Canadian Charter'), Part 1 of the Constitution Act, 1982 available at http://laws-lois.justice.gc.ca/eng/const/page-15.html (accessed on 1 November 2015).

59 Piper (n 15 above) 262.

60 ES Dove *et al* 'Charting the privacy landscape in Canadian paediatric biobanks' (2013) 20 *Health Law Journal* 13. DH Flaherty 'On the utility of constitutional rights to privacy and data protection' (1990-1991) 41 *Case Western Reserve Journal of International Law* 834. According to the author 'Canada is true to its British constitutional heritage of often avoiding the entrenchment of basic rights.' This is unlike Quebec which has an explicit provision on the right to privacy in art 5 of the Quebec Charter of Human Rights and Freedoms RSQ, c C-12. London therefore declares that Quebec has strongest provincial declaration on privacy. RW London 'Comparative data protection and security law: A critical evaluation of legal standards' unpublished LL.D thesis, University of South Africa, 2013 292.

61 See generally secs 7, 8, 2(b). See *R v Jones* (1986) 2 SCR 284. See also Piper (n 15 above) 262.

62 Unlike the US, the right to privacy is a fundamental human right in the Canadian Charter of Rights and Freedom. See Nova (n 42 above) 780. This has made commentators argue that Canadians are more concerned about their privacy than their American counterparts. See McClennan & Schick (n 29 above) 675.

63 (1984) 2 SCR 145 available at http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/5274/index.do (accessed 1 November 2015).

64 (n 63 above) 155.

65 (n 63 above) 159, he arrived at the decision relying on the US case of *Katz v. United States* US 347 (1967). However, the SCC cautioned that American decisions can only be transplanted in the Canadian context with the greatest caution. There are lots of arguments on what constitutes reasonable expectation of privacy. See generally Yusuff (n 19 above); also Department of Justice 'The offices of

section 8 is all about privacy.[66] Even though the section appears to be only applicable with respect to criminal proceedings, the Supreme Court of Canada (SCC) held in *R v Edwards*[67] that the section is equally applicable outside of the criminal law context.

With regard to the protection of data privacy specifically, the Charter has over time been interpreted by the SCC to address violation of privacy due to the collection of personal data through electronic surveillance and the use of personal data contained in databases.[68] Yet, such violation must occur only where there is a 'reasonable expectation' of privacy.[69] The case of *R v Wong*[70] is the most influential in this regard. The SCC opined in that case that unreasonable search and seizure is not dependent on the particular technology.[71] Rather, it must 'embrace all existing and future means by which the agencies of the state can electronically intrude on the privacy of the individual.'[72] What is therefore important is, whether the individual had a reasonable expectation of privacy. This is only present where an individual subjectively expected his/her information to be kept private and the subjective expectation is reasonable.[73] According to McNairm *et al,* an individual will usually have a very high expectation of privacy in respect of his/her personal information.[74] Nonetheless, it is submitted that subjecting data privacy violation to 'reasonable expectation' test is a huge limitation to the full enjoyment of the right.

---

the information and privacy commissioners: the merger and related issues' http://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/ip/p2.html#ftn5 (accessed 1 November 2015).

66 *Hunter v Southam* (n 63 above) 158,160. See Flaherty (n 60 above) 845.

67 (1996) 1 SCR 128 available at http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1340/index.do (accessed 1 November 2015). It was held by LA Forest J that the provision is '…intended to afford protection to all of us to be secure against intrusion by the state or its agents by unreasonable searches or seizure, and is not solely for the protection of criminals even though the most effective remedy will inevitably protect the criminal as the price of liberty for all'. See para 58.

68 See the cases of *R v Duarte* (1990) 1 SCR 30 and *R v Wong* (1990) 3 SCR 36. See Piper (n 15 above) 263.

69 Bailey (n 21 above) 208.

70 (n 68 above) also available at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/683/index.do (accessed 1 November 2015).

71 Relying on *R v Duarte* (n 68 above).

72 *R v Wong* (n 75 above).

73 Bailey (n 21 above) 208; In this regards, she contends that 'core biographical information' and the contents of one's personal computer attracts a reasonable expectation of privacy as they both contain intimate details about an individual. These are based on the observation in the cases of *R v Gomboc* (2010) SCC at 28 and *R v Morelli* (2010) SCC 8, at 2-3. With respect to privacy rights and content of digital devices, see *R v Fearon* (2014) SCC 77.

74 CHH McNairam *et al Privacy law in Canada* (2001) 29-30. In *R v. Plant* (1993) 3 SCR 287, the court interpreted personal information as information which 'reveal[s] intimate details of the lifestyle and personal choices of the individuals.' Thus, computer record of an individual's consumption of electricity at his residence was held to reveal little about his personal lifestyle therefore he has no reasonable expectation of privacy over it. See page 293. It is submitted that this interpretation is too narrow based on the understanding of personal information in data privacy law. See chapter 1 (1.6.3).

Other limitations are inherent in the provisions of the Charter which restricts its application in protecting data privacy (and privacy). First, Piper points out that the Charter is applicable to activities involving a government actor (not the private sector).[75] Thus, the section[76] gives individuals the right 'to assert a reasonable expectation of privacy vis-à-vis the government.'[77] However, it has been argued that private entities may trigger the application of section 8 in respect of information they hold if they become agents of the state by engaging in an activity that would not have otherwise taken place in the form and manner it did but for the involvement of the state.[78] A second limitation of the constitutional provision is that infractions can, in most cases, be justified under section 1 of the Charter as 'reasonable limitations in a free and democratic society.'[79] Once the court determines that privacy has been violated, it must ask under section 1 if limits imposed on privacy are 'reasonable' and can be 'demonstrably justified in a free and democratic society.'[80] Flaherty opines that 'such a qualification on a human right can serve as a significant barrier to successful litigation.'[81] The third limitation, as opined by Bailey, is that rights under section 8 'are only triggered in relation to information if they subjectively expected it to be kept private and that subjective expectation was reasonable.'[82]

Nevertheless, the above does not diminish the value of the right to data privacy in view of the quasi-constitutional status bestowed upon it by the courts.[83]

4.4.2. Statutory protection of data privacy

Canada, in line with international practice, has established a multifaceted but 'harmonious' legislative framework for data privacy protection which is broadly divided into the public

75 Piper (n 15 above) 263.
76 And the decision in the case of *Hunter v Southam* (n 63 above).
77 Flaherty (n 67 above) 847.
78 See Bailey (n 28 above) 208, citing *R. v M. (MR)* (1998) 3 S.C.R. 393.
79 Piper (n 15 above) 263.
80 See Flaherty (n 60 above) 845 quoting *Regina v Oakes* (1986)1 SCR 103, 104.
81 Flaherty (n 60 above) 845.
82 Bailey (n 21 above) 208.
83 This is particularly with respect to the federal laws on data privacy. See *Lavigne v Canada (Office of the Commissioner of Official Languages)* (2002) 2 SCR 773. Available at http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1994/index.do (accessed 1 November 2015). A quasi-constitutional law is a law that is not subject to overriding provisions of others. Any exemption to the application of a quasi-constitutional legislation must be explicit and narrowly interpreted. See *Nunavut (Minister of the Environment) v. WSCC* (2013) NUCJ 11. For more in-depth analysis on quasi-constitutional status of a law and its implications, See WN Eskridge & PP Frickey 'Quasi-constitutional Law: Clear statement rules as constitutional lawmaking' (1992) 45 *Vanderbilt Law Review* 593-645.

and private sectors.[84] Jennifer Stoddart declares that there is much to commend in this approach.[85] Commentators have advanced a number of reasons for the model. It is submitted, however, that this is largely due to the influence of the US and EU.[86] The US, like Canada, has historically regulated both the public and private sectors separately. The distrust of the government by the people in both countries has made them pass extensive legislation protecting personal data in the public sector. However, such distrust did not extend to the private sector especially, in the US which has been largely regulated by a patchwork system of laws and self-regulatory mechanisms. Canada also adopted a similar approach, but later, as will be seen shortly, departed from the US.[87] It must be pointed out that unlike the approach adopted at the federal level, many of the provinces regulate public and private data processing activities in the same legislation.[88]

This part of the chapter analyses the various laws for the protection of data privacy at the public and private sector with a view to identifying crucial lessons that can be learned from the Canadian experience. In this regard, a brief historical study will be carried out to unveil the mischief behind the law and the law making process.[89] Then, an analytical study will be used to examine the 'principal' substantive matters in the laws. This segment also carries out some comparative study, especially where a particular province has a provision radically different from the federal legislation. Nonetheless, it must be repeated that the

---

84 As stated in the official website of the Office of the Privacy Commissioner in Canada, a number of factors determine what law applies and which enforcement body has jurisdiction over a particular data privacy issue. They include: The nature of the organisation responsible for the personal information, the location of the organisation, they type of the information. See Office of the Privacy Commissioner of Canada 'Privacy Legislation in Canada' Fact sheets https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp (assessed 1 November 2015).

85 Stoddart (n 23 above).

86 CJ Bennett & CD Raab 'The adequacy of privacy: The European Union Data Protection Directive and the North American response' (1997) 13(3) *The Information Society* 247. The scholars opine that '… Canadian and American privacy policy have not been substantially different. Both nations have passed legislation to protect personal data held in government agencies at both federal and state/provincial levels). With the exception of Quebec, in the private sector, protection is left to a smattering of isolated statutory provisions and to voluntary codes of practice.'

87 Bennett & Raab (n 86 above), 247.

88 Some provinces even regulate public and private data processing and access to information in the same legislation. Manitoba: Freedom of Information and Privacy Protection Act; New Brunswick: Right to Information and Protection of Privacy Act; Newfoundland and Labrador, Access to personal information and protection of Privacy Act, Northwest Territories: Access to information and Protection of Privacy Act, Nova Scotia: Freedom of Information and Protection of Privacy Act; Nunavut: Freedom of Information and Protection of Privacy Act; Ontario: Freedom of Information and Protection of Privacy Act, Prince Edward Island: Freedom of Information and Protection of Privacy Act; Saskatchewan: Freedom of Information and Protection of Privacy Act; Yukon: Access to Information and Protection of Privacy Act. See Office of the Privacy Commissioner of Canada (n 84 above).

89 Especially with regard to the two primary federal laws.

whole of the chapter focuses on the legislation at the federal level only. The public sector protection of (data) privacy will now be considered.

4.4.2.1. Public sector: The Privacy Act

The Privacy Act[90] is the primary legislation regulating data processing activities of federal government departments and agencies in Canada. To depict its crucial status, the SCC has stated that the Act has a *quasi-constitutional* status.[91] With regard to provincial government agencies, every province and territory has its public sector law which is applicable and not the Privacy Act.[92]

a. The Privacy Act in historical perspective: Lessons from the law making process

A brief historical account of the Privacy Act is necessary to show where the law is coming from and what factors influence its current state.[93] The forces that propelled legislation on data privacy in the public sector are generally the same across the world: increased computerisetion of information systems and the development of unique identifiers.[94] Concerns about these issues were first raised in Canada in 1964. However, no official action was taken until 1971 when the Department of Communication and Justice established a task force on Privacy and Computers to investigate issues with computerisetion of personal information systems.[95] This task force investigated the technological impact of computers in a major federal government study titled *Privacy and computers*, in 1972 which was well received.[96] However, the task force did not make specific legislative recommendations.[97] That notwithstanding, the report provoked

---

90 Privacy Act 1985 L.R.C. (1985), ch P-21 available at http://laws-lois.justice.gc.ca/eng/acts/P-21/ (accessed 1 November 2015).

91 *Eastmond v Canadian Pacific Railway* (2004) FC 852; *Lavigne* (n 83 above). See also Bailey (n 21 above) 210 and J Stoddart 'Government accountability for personal information: Reforming the Privacy Act' available at https://www.priv.gc.ca/information/pub/pa_reform_060605_e.asp (accessed 1 November 2015).

92 See Office of the Privacy Commissioner of Canada (n 86 above).

93 For more detailed historical account, see P Gillis 'The Privacy Act: A legislative history and overview' (1987) 119 *Canadian Human Rights Yearbook* 119-147. See also DH Flaherty 'Reflections on reforms of Federal Privacy Act' (2008) https://www.priv.gc.ca/information/pub/pa_ref_df_e.pdf (accessed 1 November 2015); Bennett (n 1 above) 551.see also Department of Justice (n 65 above).

94 Bennett (n 1 above) 555.

95 Bennett (n 1 above) 555, Department of Communication and Department of Justice *Privacy and computers*, A report of a Task Force established jointly by the Department of Communications/ Department of Justice (1972).

96 See N Holmes 'Canada's federal privacy laws' (2008) http://www.parl.gc.ca/Content/LOP/researchpublications/prb0744-e.htm (accessed 1 November 2015). See also Gillis (n 93 above) 122.

97 Bennett (n 1 above) 555.

extensive debate on data privacy in Canada.[98] Accordingly, the Federal government appointed an Interdepartmental Committee on Privacy to prepare a federal privacy law.[99] The Canadian Human Rights Act of 1977[100] was the first legislation in this regard. Part IV of the Act contained a set of fair information principles (FIPs) for the public sector and it also established the Office of the Privacy Commissioner as an ombudsman.[101] Part IV 'institutionalized the Office of the Privacy Commissioner; and it energized the Treasury Board, authorised to oversee the information policy of the federal government.'[102] The flaws in this law with regard to privacy protection became apparent over time.[103] However, this was not sufficient to cause an amendment of the Human Rights Act.[104] The immediate cause for legal reforms was a parallel debate on access to government information which generated more public controversy than the privacy debate.[105] In 1980 therefore, a comprehensive law addressing both issues was brought before parliament.[106] The Bill (Bill C-43) contained both the present Access to Information Act and the Privacy Act and it came into force on 1 July 1983.[107] It effectively replaced the Canadian Human Rights Act.[108]

Francis Fox (the then Minister of Communications) saw Bill C-43 through the parliament.[109] Barry Strayer, Stephen J. Skelly, QC, and Gillian Wallace, QC, all experienced justice specialists were the brains behind processes leading up to the Act.[110] These officials, according to Flaherty, were 'policy entrepreneurs in what privacy

98 Bennett (n 1 above) 558.
99 Bennett (n 1 above) 558.
100 Received royal assent in July 1977 and became operational in March 1978.
101 Bennett (1 above) 558.
102 Bennett (n 1 above) 559.
103 The flaws of this law became more apparent with the growth of privacy principles and standards outside Canada in the US and Europe. Gillis (n 93 above) 125. According to Bennett, '[m]ost of the Canadian Human Rights Act is devoted to the question of discrimination. Privacy principles were included with very little debate, and with little public reaction' (n 1 above) 559. See also Holmes (n 96 above) 2 where she contends that '[a]rguably, the anti-discrimination provisions of the Canadian Human Rights Act were not the best fit for the right to privacy.'
104 Gillis (n 93 above) 125.
105 Gillis (n 93 above) 125, Bennett (n 1 above) 559.
106 Department of Justice (n 65 above).
107 Several comments however show how the debate for the Access to Information Act overshadowed that of privacy and made privacy a bit neglected. Anyway, the Bill passed its second reading on 29 January 1981 and was sent to the Standing Committee on Justice and Legal Affairs. Bill C43 was finally sent to the house on 28 June 1982 for its third reading. See Bennett (n 1 above) 560; Holmes (n above 103) 2; Department of Justice (n 65 above).
108 See *Lavinge* (n 83 above); see also *Canada (Privacy Commissioner) v Canada (Labour Relations Board)* (1996) 3 FC 609 at 652.
109 Flaherty (n 93 above).
110 Flaherty (n 93 above).

advocates would regard as the best sense of them.'[111] They also constituted part of 'a specialised international movement in advanced industrial societies that, for example, produced the highly-influential Organisation for Economic Cooperation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980) ['OECD Guidelines'].'[112] Flaherty further observes that '[t]he key roles of these politicians and public servants is a reminder that a committed cadre of subject-matter specialists is instrumental to both the introduction and further revision of any single piece of [data] privacy legislation.'[113] The political will in the subject matter also had a crucial role to play. This brief historical account reveals three important lessons. First, the process leading up to the Act was a gradual and careful process with sufficient research, debates and consultation. Second, is the presence of strong political will and the third, is the role of experts in the law-making process. Other lessons can be drawn from the substantive provisions of the law.

b. Purpose of the Privacy Act

The Act has two broad objectives: it seeks 'to extend the present laws of Canada that protect privacy of individuals with respect to personal information about themselves held by a government institution' and also to 'provide individuals with a right of access to personal information about themselves'.[114] The first stated objective establishes the relationship between data privacy and privacy and unequivocally shows the 'added value' of data privacy law.[115] This objective is also an acknowledgement of the weaknesses of the constitutional and common law protection of personal data which is a reason for the extension of the extant framework on privacy. Nevertheless, the objective is very narrow with respect to the general objectives of a law on data privacy today. There is no word in the objective of the Act suggesting that the processing of personal data threatens human

111 Flaherty (n 93 above).

112 Flaherty (n 93 above). See also Organization of Economic Cooperation Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) ('OECD Guidelines') available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 1 November 2015).

113 Flaherty (n 93 above).

114 Privacy Act, long title & sec 2; See also the case *Lavinge* (n 83 above).

115 See O Lynskey 'Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order' (2014) 63 *International and Comparative Law Quarterly* 569-597 for more elaborate discussion on the added value of a data privacy.

rights of individuals and as such, the law must protect such rights in an age of massive and sophisticated data processing activities by the government. [116]

c. Jurisdiction and application of the Act

The scope of legislation on data privacy is usually considered from three perspectives: the scope with regard to the type of data; type of data processing and sectors (main players).[117] The Privacy Act does not outline the scope of the law. Nevertheless, it is implicitly provided in certain provisions. With respect to the type of data, section 2 provides that the Act protects the privacy of individuals with respect to 'personal information'. Personal information is in turn defined under section 3 as 'information about an identifiable individual that is recorded in any form.' Personal information within this provision includes a wide range of data like information relating to race, nationality or ethnic origin, colour religion, age, marital status, identifying number, address, and finger print.[118] The Act, however, provides for certain instances where personal information will not fall within its scope. This is largely for the purpose of realising some of the objectives of the Access to Information Act.[119] Two important observations are worthy of note with respect to the scope of the Privacy Act as regards the type of data. The first is that it narrowly applies to personal information in recorded form which, for the purpose of data privacy law, is only personal information that is stored and not necessarily personal data that is

---

116 Eg, art 1 of the EU Directive provides that 'in accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'

117 As adopted by LA Bygrave *Data protection law: Approaching its rationale, logic, and limits* (2002) 41-56; See also Elder (n 12 above) 44. His classification of scope is: main players (sectors); types of data; and type of acts/operations.

118 Privacy Act, sec 3. In *Dagg v Canada (Minister of Finance)* (1997) 2 SCR 403, the court interpreted personal information broadly to include any information about the identity of the person. Surprisingly, in a subsequent case of *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation & Safety Board)* 2006 FCA 157 (CCA), the Federal Court of Appeal gave a rather narrow interpretation that 'privacy thus connotes concepts of intimacy, identity, dignity and integrity of the individual'. See B McIsaac *et al The law of privacy in Canada* (2011) 3-7.

119 Thus for the purposes of sec 7, 8, 26, and 19 of the Access to Information Act, information about an individual who is or was an officer or employee of a government institutions that relates to the position or functions of the individual is not personal information under the privacy Act. Such information include the fact that the individual is or was an officer or employee of a government institution, the title, business address and telephone number of the individual, classification, salary range and responsibilities of the position held by the individual etc. Other exceptions as a result of certain provisions in the Access to Information Act are contained in sec 3.

collected, disclosed or transmitted. Secondly, the definition does not distinguish between sensitive and non- sensitive data as many current data privacy laws do.[120]

Obviously, with respect to the type of data processing, the Act only applies to recorded personal information. This can be inferred from the provisions of section 2.[121] Nevertheless, there are numerous provisions specifically applicable to the collection and disclosure or use of personal information. As has been stated earlier, the Privacy Act applies only to federal government agencies and institutions listed out in the Schedule of institutions contained in the Act.[122] This is the scope with respect to the sectoral coverage.[123]

d. Fair information principles (FIPs)

The FIPs in the Privacy Act are not outlined in a specific section like in most data privacy legislation. A number of them (FIPs) can, however, be deciphered from the various provisions of the law.[124] With respect to the *processing limitation or limitation of collection principle* which is a fundamental principle of data privacy law, section 5(1) provides that a government institution must only collect personal information that is intended to be used for administrative purposes directly from the individual to whom it relates.[125] There are two exceptions to this principle: 'where the individual authorizes otherwise or where personal information may be disclosed to the institution under subsection 8(2).'[126] This principle, though not contained in the EU Directive, is very crucial as it is the primary way an individual may know that his/her information is being processed and grant or withhold consent as the case may be. The principle is, however, narrow in that it relates to only collected personal information for 'administrative purpose' which is defined as the use of personal information 'in a decision making process that directly affects that individual.'[127] It therefore presents a bizarre situation where there is no

120 See eg, art 8 EU Directive.
121 And from the title of the Act.
122 As of 16 February 2015, the Act applies to over 200 government institutions. See Privacy Act, schedule (sec 3) Government Institutions http://laws-lois.justice.gc.ca/eng/acts/P-21/page-25.html#h-35 (accessed 1 November 2015).
123 There are certain other situations where the Act does not apply for example, library or museum material preserved for public reference, and material placed in library and archives of Canada etc. Sec 69 & 70.
124 Bygrave acknowledges this approach of providing for the principles as fully fledged legal rules on their own in their own right. Bygrave (n 38 above) 145. See also Bennett & Raab (n 10 above) 12.
125 Privacy Act, sec 5 (1).
126 Privacy Act, sec 5 (1).
127 Privacy Act, sec 3.

need to collect personal information directly from the individual if it is to be used for other purposes short of 'administrative purpose'.

The *purpose specification* principle is partly provided for in section 4. The Act provides that '[n]o personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.'[128] It is submitted that the 'operating program or activity of the institution' should be in accordance with the establishing statute of the government agency. Thus, an institution is not allowed to collect personal information for purposes outside its operating program or activity as such will run afoul of the purpose specification principle. Nevertheless, Klein argues that 'the requirement that the information relate directly to an operating program or activity of the institution is arguably very little protection from what could be the indiscriminate collection of personal information.'[129] This is because 'it is easy to justify collection of personal information in many instances.'[130] Section 4 seems also to provide for the *use limitation* principle as personal data cannot be used contrary to a specified purpose or scope of the government agency. Section 5(2) is more direct on the purpose specification principle. It provides that '[a] government institution shall inform any individual for whom the institution collects personal information about the individual of the purpose for which the information is being collected.' Section 5(2) and (1) do not apply where specifying purpose or collecting directly from the individual may result in the collection of inaccurate information or defeat the purpose for which information is collected.[131]

Section 6(1), which provides for the retention of personal information used for an administrative purpose, is another aspect of the purpose specification principle. In terms of the Act, '[p]ersonal information that has been used by a government institution for an administrative purpose shall be retained for such period of time after it is so used…to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information.'[132] It is further provided that a government institution should dispose of personal information under its control 'in accordance with the regulations and in accordance with any directive or guidelines issued by the designated minister with respect

128 Privacy Act, sec 4.
129 Klein (n 32 above) 69.
130 Klein (n 32 above) 69.
131 Privacy Act, sec 5(3).
132 Privacy Act, sec 5(3) & sec 6.

to disposal of that information.[133] This has a similarity with the modern day right to delete or the right to be forgotten. A fine distinction can, however, be maintained between section 6(3) and the right to delete (as conceived under the EU data privacy instruments). The former requires a positive action from the individual, unlike the latter which is an obligation on a government institution independent of an individual.[134] Be that as it may, the section places an unduly restrictive condition for the disposal in that it has to be in accordance with regulations, directives or guidelines issued by the minister.[135] This gives the minister too much discretionary power with regard to personal information.

With respect to the *data quality* principle, section 6(2) provides that 'a government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.' The *use limitation* principle seems to be more explicitly stated in section 7. In terms of the Act personal information under the control of a government institution must not be used without the consent of the individual to whom it relates except for the specified purpose or 'use consistent with that purpose'[136] or for a purpose for which the information may be disclosed to the institution under section 8(2). Section 8 generally provides for rules on disclosure of personal information by a government institution. In terms of the Act, personal information must only be disclosed if the individual to whom it relates consents, except in circumstances under section 8(2) which include for a specified purpose or 'a use consistent with that purpose'[137] and in accordance with an Act of Parliament or any regulation. The concept of 'consistent use' in section 8(2) has been a particularly controversial concept. In *Re Canada (Privacy Commissioner),*[138] the Federal Court of Appeal held that section 8(2) shows a clear intention of Parliament to allow non-

133 Privacy Act, sec 5(3), sec 6 (3).

134 See generally PA Bernal 'A right to delete?' (2011) 2 *European Journal of Law and Technology* available at http://ejlt.org/article/view/75/144 (accessed 1 November 2015).

135 Privacy Act, Sec 6 (3).

136 Privacy Act, sec 7(a).

137 The concept of 'consistent use' has come before the court in *(Privacy Commissioner)*, Re 2000 CarswellNat 1756 (C.A.). (Cited in Klein (n 39 above) 71. Revenue Canada has a practice of releasing personal data on travellers to another government agency, the Canada Employment and Immigrations Commission, so as to enable the latter to apprehend those receiving unemployment insurance benefits while out of the country. The main issue for consideration was whether the disclosure by Revenue Canada of this information was authorised by the sec 8(2) of the Privacy Act. The Federal Court of Appeal held that the section was a clear intention by parliament to allow non-consensual disclosures of personal information, including for other purposes than those for which the information was collected. On the contrary, in *B(A) v Canada (Minister of Citizenship and Immigration)* (2002) FCJ 610 'consistent use' was narrowed as the court held that an administrative tribunal could not release personal information in the forms and transcripts of one of its hearing for use in separate hearings.

138 *Re Canada (Privacy Commissioner)*Re 2000 CarswellNat 1756 (C.A.).

consensual disclosures of personal information, including for other purposes than those for which the information was collected. The court gave a hint on how wide the 'consistent use' concept could be used to justify disclosure of personal information.[139] Nevertheless, Gillis points out that government policy directs that consistent uses must have 'a reasonable and direct connection' to the original purpose of collection.[140] It is submitted that the phrase 'reasonable and direct connection' is too vague and leaves too much to the discretion of a head of the institution. Subsection (f) of the section is particularly problematic, as it provides a situation where individuals' personal data may be disclosed to 'the government of a foreign state, an international organization of states or an international organization established by the governments of states' for the purpose of administering or enforcing any law or carrying out a lawful investigation'.[141] This section particularly puts individuals' at so much risk.

The forgoing is as far as the Act provides for the FIPs. Traces of the *openness or transparency principle* can, however, be seen in section 11 which obliges the designated minister to publish an index of all personal information banks setting forth certain details to enable easy access by individuals.[142] Though not explicitly provided for in the Act, it could be argued that the *accountability principle* is also contemplated as Gillis contends that the head of each government institution is responsible for administration of the Act in that institution.[143] If this argument is accepted, then it implies the existence of the *accountability principle*. This is because 'the head of the institution is directly accountable for carrying out these responsibilities, but they can be delegated to one or more officers of the institution.'[144]

e. Rights of individuals and duties of government organisations

The Privacy Act also provides for certain rights which relates to the overall objective of a data privacy law. All Canadian citizens or permanent residents have a right to and shall be given access to their personal information contained in a personal information bank.[145] This also includes 'any other personal information about the individual under the control

139 *Re Canada (Privacy Commissioner)* (n 138 above).
140 Gillis (n 93 above)131.
141 Privacy Act, sec 8(2)(f).
142 The Publication is called *Info Source* see Klein (n 32 above) 71.
143 Gillis (n 93 above) 143.
144 Gillis (n 93 above) 143.
145 Privacy Act, sec 12.

of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it retrievable'.[146] It is submitted that this provision is unduly restrictive of an individual's right of access in two respects. Firstly, the section grants access to only certain category of persons (Canadian citizens and permanent residents and not non-citizens) and secondly, it unreasonably places a burden on an individual to provide facts not within his/her control.

Other rights bestowed on individuals by the Act pursuant to the right of access are the right to request correction of the personal information where he/she believes there is an error or omission and the right to require that a note be attached to the information reflecting any correction requested but not made.[147]

f. Exemptions and qualifications

Bennett opines that the Privacy Act contains two sets of exemptions to the FIPs:[148] Those relating to individual access and those relating to disclosure of information to other organisation.[149] Apart from the general provisions which restrict individuals' access to their personal data discussed above,[150] wide powers are given to the Governor in Council to designate certain personal information banks containing personal information as exempt banks.[151] Information contained in an exempt bank is completely inaccessible 'because it is information that was obtained or prepared by any government institution, or part of government institution, that is an investigative body specified in the regulations in the course of lawful investigations pertaining to the enforcement of any law of Canada or a province'.[152] Thus, the head of a government institution may refuse to disclose personal information based on a right of access if such information is contained in an information bank designated as an exempt bank.[153]

Similarly, section 19 grants the head of a government institution the power to refuse the disclosure of any personal information based on a right to access if such information is

146 Privacy Act, sec 12 (b).
147 Privacy Act, sec 12 (2)(a) and (b). Subsec 3 provides for a minor right for extension of right of access by order.
148 Bennett (n 1 above) 563.
149 These exceptions have already been considered under the FIPs above
150 In the discussions on the FIPs.
151 Privacy Act, sec 18(1).
152 Klein (n 32 above) 77.
153 Privacy Act, sec 18 (2).

obtained in confidence from several sources outlined in the section.[154] It is submitted again, that this exemption is too wide, unwarranted and unduly restricts the rights of individuals. Several other instances where the head of a government institution and Privacy Commissioner shall refuse to disclose personal information are also provided for.[155]

Apart from this main legislation (i.e. Privacy Act), several other laws (existing and pending) have placed restrictions on the provisions of the Privacy Act especially for national security purposes. This is why the Privacy Commissioner (together with provincial Privacy Commissioners) has always advocated for a 'balanced legislative approach' in legislating for national security issues.[156]

g. Transborder data flow regime under the Privacy Act

The Act does not contain any provision which regulates transborder data flows or inter-provincial data flows.[157] What this means is that personal data that is transferred from one government agency to another entity outside Canada or an entity in another province has no form of protection. This is against the general trend of legislating for data privacy and has been criticised.[158] Perhaps this is the reason why the Treasury Board of Canada[159] issued a policy which requires government agencies to ensure 'that appropriate privacy protection clauses are included in contracts or agreements that may involve intergovernmental or transborder flows of personal information'.[160] It is, however, submitted that this non-binding regime of transborder data flow (TBDF) cannot be an effective substitute for proper statutory provisions especially in terms of implementation and enforcement.

---

154 Privacy Act, sec 19(1).

155 Privacy Act, sec 21-28.

156 According to the Privacy Commissioner, 'a balanced legislative approach would also, in my view, include in Bill C-44 measures to make the activities of all federal departments and agencies involved in national security subject to independent oversight.' D Therrien 'Senate standing committee on National Security and Defence (SECD) on Bill C-44, An Act to amend the Canadian Security Intelligence Service Act and other Acts' https://www.priv.gc.ca/parl/2015/parl_20150309_e.asp (accessed 1 November 2015).

157 McClennan & Schick (n 29 above) 675.

158 Klein (n 32 above) 85.

159 'The Treasury Board President is the designated minster responsible for preparing policy instruments concerning the operation of the Privacy Act and its Regulations.' Treasury Board of Canada Secretariat Policy on Privacy Protection http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=HTML (accessed 1 November 2015).

160 Treasury Board of Canada Secretariat (n 159 above), sec 6.2.11.

4.4.2.2. A critique of the Privacy Act: Lessons from a 'not so good' example?

The Privacy Act has made some efforts in protecting data privacy rights in Canada's federal public sector. It contains far-reaching provisions on access to personal information in information banks of federal government parastatals, however, there are quite a number of criticisms of the Act largely as a result of its age.[161] Commentators argue that the Act was sufficient when the main data privacy issue was manual information collection and storage.[162] The law may find it difficult to cope with the challenges of contemporary hi-tech data processing activities and advancing government surveillance programs today.[163] With all these issues, the question remains whether lessons could be drawn from the substantive provisions of the Privacy Act. It is submitted that there are certainly lessons to be drawn from a 'not so good' example by any country developing a framework on data privacy. Thus, some observations on the substantive provisions are vital at this point.

With respect to the substantive provisions, the Act falls short in some aspects.[164] The Privacy Act has a narrow scope which makes it restricted in protecting the right to data privacy. Regarding the scope of the law as regards the type of data, it applies to only personal information in a recorded form.[165] In this researcher's view, information in a recorded form means only personal information which is stored.[166] This means the collection and use of personal data is not a data privacy issue which the Act really bothers about. Though, the definition of personal information shows it is applicable to only recorded information, there are several provisions in the Act on the collection and use of

---

161 See generally Flaherty (n 93 above). While there are many minor amendments to the Privacy Act over the years, it remains substantially unaltered. See also Klein (n 37 above) 67.

162 The Act has not been substantially modified. '[t]his is significant when you consider the changes to government programs over the years, the growth of those programs, the move from paper-based information collections to electronic storage information, the sheer proliferation of information collection done by government and the newfound importance and value of personal information' Klein (n 32 above) 67.

163 The Privacy Commissioner of Canada in an Annual report to Parliament as far back as 2004 states that '[t]oday's commonplace information technologies- the internet and new surveillance technologies such as digital video, linked networks, global positioning systems, black boxes in cars, genetic testing, biometric identifiers and radio frequency identification devices (RFIDs) – did not exist when the Federal Privacy Act came into force in 1983. Characterizing the current Act as dated in coping with today's realities is an understatement- the Act is tantamount to a cart horse struggling to keep up with technologies approaching warp speed' See Privacy Commissioner of Canada, Annual Report to Parliament, 2004-2005, http://www.privcom.gc.ca/information/ar/200405/200405_pa_e.asp (accessed 1 November 2015).

164 The critique of the Privacy Act in this segment will be restricted to its provisions on substantive matters especially related to the FIPs. Issues of enforcements will be discussed shortly.

165 Privacy Act, sec 2.

166 A dictionary meaning of the word record is to set down or register in some permanent form. J Pearsall (ed) *The oxford concise dictionary* (1999).

personal data.[167] It is submitted, therefore, that there is an inconsistency between the scope on the type of data and data processing activities. Normally, laws on data privacy usually cover a wide range of data processing activities which make Kuner opine that it is difficult to conceive of any operation performed on personal data which will not be covered by the word 'processing'.[168]

It is also noteworthy that the Act does not distinguish between personal information that is sensitive and non-sensitive. Data privacy laws usually distinguish between them and provides for a special regime on the processing of sensitive information. Such category of personal data is usually given enhanced protection.[169] This approach may be criticised on the basis that the processing of personal information that will subject an individual to more risk deserves more protection. It is, however, submitted that such an approach has its merits in that personal data that is not otherwise sensitive (like a person's name), may become sensitive when used in certain circumstances or combined with other personal information. Consequently, it is arguable that all personal information deserve equal protection and the approach of the Privacy Act has its advantages.

Certain FIPs are not explicitly stated in the Act. For example, the Act does not have a general provision on *fair and lawful processing* which is said to be 'the primary principle of data privacy law'.[170] The fair and lawful processing principle 'embraces and generates the other privacy principles'.[171] The Act also does not contain the *safeguard* and *accountability* principles. This brings about some difficulties because of the provision that requires that the head of a government institution that processes personal data must establish a personal information bank containing 'all personal information under the control of the government institution'.[172] There is no provision for security safeguards of such personal data in the data bank and there is equally no requirement that a particular

---

167 For eg, secs 4-6; 7, 8.

168 C Kuner *European data protection law: Corporate compliance and regulation* (2007) 74. Bygrave also notes that 'current data privacy laws typically regulated all or most stages of the data-processing cycle, including registration, storage, retrieval, and dissemination of personal data.' (n 45 above)141.

169 See for eg, art 8 EU Directive. This approach is called a purpose-based approach as against a contextualised approach. The approach of the Privacy Act and the PIPEDA, the German and Australian data protection regime, is a contextualised approach. Whether personal information is considered sensitive or not depends on the context of the processing. See R Wong 'Data protection online: Alternative approaches to sensitive data? (2007) 2(1) *Journal of International Commercial Law and Technology* 9-16.

170 Bygrave (n 38 above) 146, this is not surprising however since the Act is substantially based on the OECD Guidelines which does not contain this principle.

171 Bygrave (n 38 above) 146.

172 Privacy Act, sec 10.

government official is accountable for the security databanks. This places the vast quantity of personal data contained in such databanks at great risk.[173]

An analysis of the Act also shows that there are too many exemptions granted to various heads of government institutions for the processing of personal data.[174] Some are particularly extreme and put individuals at risk. For example, in outlining instances where personal information may be disclosed without consent of the individual, section 8(2)(f) permits personal information to be disclosed to a foreign government or international organisation for law enforcement purposes. This provision is worrisome considering that the Act has no special regime on transborder data flows. Similarly, many provisions give the head of a government agency very wide discretionary power on compliance issues.[175] Finally, the Act is too long and contains many archaic and irrelevant provisions. Also, it creates too many bureaucracies which can stand in the way of individuals enjoying their right of access to their personal data in the hands of government agencies.[176]

In spite of the old-fashioned nature of the Privacy Act, the Canadian legal system has devised means to ensure 'sound management practices' with respect to the handling of the protection of personal information under the Privacy Act regime. This was done by the issuing of the Policy on Privacy Protection, in 2014 by the Treasury Board of Canada,[177] which among others is 'to facilitate statutory and regulatory compliance, and to enhance effective application of the Act and its regulations by government institutions.'[178] This policy was developed in consultation with the Privacy Commissioner's office.[179] The Treasury Board ensures compliance with the policy through various strategies.[180] The

---

173 The closest to safeguard of personal data contained in the Act is sec 25 (1) which provides that '[T]he head of a government institution may refuse to disclose any personal information requested under subsection 12(1) the disclosure of which could reasonably be expected to threaten the safety of individuals.'

174 See eg, secs 18 and 19.

175 See eg, sec (2) (m).

176 Eg, see secs 13-17. Also too many institutions are responsible for administering the Act. Eg, Privacy Commissioner and his/her delegates, the courts, the minister in charge of administering the legislation, i.e. the President of the Treasury Board etc.

177 See Treasury Board of Canada (n 159 above).The Treasury Board is responsible for accountability and ethics, financial, personnel and administration management etc. The President is the head of the Treasury Board and he manages the government by translating the policies and programs approved by the cabinet into operational reality. See Treasury Board of Canada Secretariat 'About the Treasury Board' http://www.tbs-sct.gc.ca/tbs-sct/abu-ans/tb-ct/abu-ans-eng.asp (accessed 1 November 2015).

178 (n 159 above), sec 5.1.1.

179 Stoddart (n 23 above).

180 Eg, sec 7.1 of the policy provides that those government institutions that do not comply will be required by the Treasury Board 'to provide additional information relating to development and implementation

major problem with this policy is its non-binding nature because it is not a legal document *stricto sensu.*

It is also important to point out that the fact that the Act has some lapses does not mean that the personal information of Canadians is largely unprotected in the public sector. Such limitations only exist in the federal public sector as various provincial data privacy legislation have set far better standards than the federal law.

4.4.2.3. Private sector: The Personal Information Protection and Electronic Documents Act (PIPEDA)

The PIPEDA is the most recent legislative effort to protect data privacy right at the federal level in Canada.[181] It is the primary legislation on the private sector in Canada. There are also several sectoral laws.[182] Nevertheless, 'the presence of other legislation that has privacy-related provisions does not necessarily mean that PIPEDA does not apply.'[183] The PIPEDA is recognised as a fundamental law of Canada and as such enjoys a quasi-constitutional status.[184]

a. The PIPEDA in historical perspective: Lessons from the law-making process

As stated above, Canada and the US regulated the collection and use of personal information in a similar way with extensive laws regulating public sector processing of personal data.[185] Both countries left the private sector unregulated.[186] With time, however, there was a general trend in some North American countries to begin regulation of private sector processing of personal data through laws. Berzins identifies four key developments

---

of compliance strategy in their annual report to parliament. This reporting will be in addition to other reporting requirements and will relate specifically to the compliance issues in question.'

181 PIPEDA S.C. 2000, c 5. Available at http://laws-lois.justice.gc.ca/eng/acts/p-8.6/ (accessed 1 November 2015). Piper (n 15 above) 255.

182 Like the Federal Bank Act. See Office of the Privacy Commissioner of Canada (n 84 above).

183 Office of the Privacy Commissioner of Canada (n 84 above).

184 This is because the right to data privacy is taken as a fundamental right in Canada. See *Eastmond v Canadian Pacific Railway* (n 91 above); *Lavigne v Canada* (n 83 above).

185 However, an area of divergence is the creation of the Office of the Privacy Commissioner to oversee the Canadian Privacy Act. Moshell states that 'with the exception of establishing the Office of the Privacy Commissioner, the Canadian Privacy Act contained many provisions similar to those found in the United States Privacy Act of 1974' (n 31 above) 422.

186 Quebec, however, had extensive legislation on data privacy in the private sector. For more succinct analysis on the divergence between the Canadian and US policy on privacy, see Bennett & French (n 30 above).

which are responsible for this.[187] The first, which he refers to as 'the most critical factor', has been the emerging recognition of the threats posed by the private sector.[188] Across the world, it was realised that the processing of personal data by commercial entities poses similar threats to individuals' data privacy as that of the government. This was not always the case as the state, with its surveillance capabilities, always used to be the subject of concern. The second reason for the adoption of private sector laws was the influence of the development of international consensus on FIPs which became widely accepted and did not distinguish between public and private sectors.[189] The increasing difficulty to distinguish between public and private use of personal information is the third reason for private sector regulation.[190] Finally, the influence of the EU and its 'adequacy requirement' for TBDF also influenced regulation of the private sector by the North Americans.[191]

Before enacting the PIPEDA, the private sector had always been regulated by voluntary codes in Canada.[192] A considerable number of sectoral codes were developed in the 1990s, largely to discourage the government from passing a legislation in that sector.[193] The Canadian Standards Association (CSA) began consultations which culminated in the Model Code for the Protection of Personal Information in 1996 (CSA model code).[194] This code was soon to become a very influential force in Canadian private sector data privacy regime. The CSA's effort was significantly influenced by international developments in Europe, especially by the EU Directive.[195] The ensuing CSA model code was successful as it was arrived at by a consensus of business representatives, consumer advocates, privacy

187 C Berzins 'Protecting personal information in Canada's private sector: the price of consensus building' (2001-2002) 27 *Queen's Law Journal* 615.

188 Berzins (n 187 above), 615.

189 Berzins (n 187 above) 615-617.

190 Berzins (n 187 above) 617.

191 Berzins (n 187 above), 618; McIsaac (n 118 above) 4-4.

192 See CJ Bennett 'Adequate data protection by year 2000: The prospects for privacy in Canada' (1997) 11 *International Review of Law and Computers* 87. See also CJ Bennett 'Protecting privacy on the Canadian information highway: policy developments and regulatory options' (1996) 21(3-4) *Canadian Journal of Information and Library Science* 3-7.

193 The private sector still wanted to avoid government overarching privacy legislation like the US. Berzins (n 187 above) 619.

194 Holmes (n 96 above) 3; D Lithwick 'Bill S-4: An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act (2014) 1 http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/2/s4-e.pdf (accessed 1 November 2015).

195 Lithwick (n 194 above) 1; especially the 'adequacy requirement' in the EU Directive. Berzins (n 187 above) 620.

experts, and representatives from the Office of the Privacy Commissioner.[196] Similarly, the Code became a 'substantive core' of the ensuing legislation (the PIPEDA).[197]

Though the Code has some measure of success, it had to give way to a law by Parliament. The main reason for this was that it had no provision on oversight and enforcement which did not go down well with international prescripts on data privacy.[198] The government was also committed to 'an electronic commerce strategy' which was intended to make Canada a world leader in e-commerce.[199] Voluntary codes will absolutely not meet the requirement of the EU, which was imperative for the flourishing of e-commerce in Canada. Therefore, after considerable debate, legislation on the collection, use and disclosure of personal information in Canadian Private Sector, the PIPEDA was enacted.[200]

Be that as it may, an important point to note for the purpose of lesson-drawing is that at some point in the negotiation process of the model code (which was subsequently integrated into the PIPEDA), Industry Canada consulted Ian Lawson, a renowned privacy expert, to carry out a comprehensive study of the regulatory options available for the protection of privacy.[201] The study relied heavily on comparative evidence and analysis and it reviewed extensive options available.[202] Similarly, Colin Bennett was asked to assess the oversight and enforcement mechanism that was most suitable.[203] Both experts' studies informed the discussion paper released by Industry Canada in 1998.[204] This discussion paper drew heavily from the works of experts in data privacy such as Flaherty.[205]

196 Berzins (n 187 above) 620.
197 Berzins (n 187 above) 621.
198 Berzins (n 187 above) 621.
199 McIsaac (n 118 above) 4-3.
200 Berzins (n 187 above) 610. It received royal Assent on April 13, 2000 and came into force on January 1, 2001. It adopted a phased implementation strategy and by 2004, it was made to apply to all the private sector except provinces with substantially similar laws.
201 Berzins (n 187 above) 624. See I Lawson 'Privacy and the information Highway, Regulatory options for Canada' (1996).
202 Berzins (n 187 above) 624; Lawson (n 201 above).
203 Berzins (n 187 above) 624, see Bennett's study 'Regulation Privacy in Canada: An analysis of oversight and enforcement in the private sector' (1996).
204 Berzins (n 187 above) 624, C Bennett 'Protection of personal information: Building Canada's information economy and society' (1998).
205 Berzins (n 187 above) 624

b. Purpose of the PIPEDA

The main objective of the PIPEDA is to 'support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances.'[206] This objective presents the PIPEDA as an instrument for the facilitation of commerce. Nevertheless, section 3 provides that the PIPEDA seeks to 'establish … rules to govern the collection, use and disclosure of personal information in a manner that *recognizes the right of privacy of individuals* with respect to their personal information and the need for organisations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate.'[207] This section shows the two broad agenda of the PIPEDA: to protect privacy of individuals with respect to their personal information and the need for organisations to be able to lawfully use this personal information. A balancing technique is therefore adopted by the Act.

c. Jurisdiction and application of the Act

Part 1 of PIPEDA applies to every organisation that collects, uses or discloses personal information in the course of 'commercial activities' or every organisation that collets, uses or discloses its employees, personal information 'in connection with the operation of federal work, undertaking or business.'[208] Personal information is defined as 'information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.'[209] Thus, the PIPEDA protects personal information as narrowly construed and personal health information.[210]

The foregoing shows that the PIPEDA applies only to the collection and use of personal data in the course of commercial activities. Commercial activity has been defined as 'any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or

---

206 PIPEDA, title

207 (Emphasis added). PIPEDA, sec 3. See *Englander v Telus Communications Inc* (2004) FCA 387 (CanLII) para 38 also available at http://www.canlii.org/en/ca/fca/doc/2004/2004fca387/2004fca387.html (accessed 1 November 2015).

208 PIPEDA, sec 4(1).

209 PIPEDA, sec 2. Quebec's law defines personal information as any information about a natural person that allows that person to be identified. It is my view that both definitions seek to achieve the same purpose i.e. exclude legal or corporate persons from the scope of the law.

210 Personal health information is information concerning physical or mental health, health service provided, donation of body part, information collected in the course of providing health services or incidental to provision of health service of an individual. PIPEDA, sec 2.

other fundraising lists.'[211] Thus, the Act is not applicable to organisations not engaged in commercial activities like non-profit charity groups, associations, and political parties.[212] This restriction is, according to London, a major constraint[213] and has been the subject of many debates.[214] The question is whether a non-profit organisation can be involved in commercial activity? Stefanick points out that the jurisprudence from the Office of the Privacy Commissioner shows a form of 'coverage creep' to apply to not-for-profit organisations that engage in commercial activities.[215] For example, in 2010 the Privacy Commissioner of Alberta recommended that a non-profit recreation facility comply with the relevant privacy statute because it sold beverages to patrons. Such activity was considered a 'commercial activity'.[216]

Nevertheless, it has been held that an organisation's taxable status is relevant to determine whether or not an organisation is engaged in a commercial activity.[217] Information gathering by an organisation in preparation for a civil tort action has been held not to be a commercial activity, even when a third party (a private investigator) is engaged to collect personal information.[218] In a more insightful approach, Quebec's privacy law, rather than apply the 'commercial activity' criterion, provides that it applies to every organisation 'carrying on an enterprise'[219] This approach appears to be wider than the PIPEDA as it applies a broad definition to organisations who are not necessarily profit-making ventures.

With respect to the geographical scope, the 'PIPEDA sets out the ground rules for how private-sector organisations collect, use or disclose personal information in the course of

---

211 PIPEDA, sec 2. Spaeth *et al* opine that the PIPEDA's definition of commercial activity is wide enough to cover almost all forms of commercial activity. JM Spaeth *et al* 'Privacy, Eh! The impact of Canada's Personal Information Protection and Electronic Documents Act on transnational business' (2002) 4 *Vanderbilt Journal of Entertainment Law and Practice* 33. See *Montana Band of Indians v. Canada (Minister of Indian and Northern Affairs)* (1989) 1 FC 143, 153.

212 Office of the Privacy Commissioner (n 84 above).

213 London (n 60 above) 274.

214 Klein (n 32 above) 27.

215 Stefanick (n 10 above) 41.

216 Stefanick (n 10 above) 41.

217 Klein (n 32 above) 27 citing *Rodgers v. Calvert* (2004), 2004 CarswellOnt 3602 (SCJ). Similarly, it was held that mere contractual relationship between two parties involving an exchange is not a commercial activity.

218 *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 FC 736 (CanLII) cited in Klein (n 39 above).

219 An Act Respecting the Protection of Personal Information in the Private Sector, Chapter P- 39.1, Quebec; sec 1 available at http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html (accessed 1 November 2015). BC Keith 'Privacy north of the border: 10 things you should know about Canadian personal information laws' (2004) 14 *American Business Association Business Law Section.*

commercial activities across Canada.'[220] The Act applies to provincial commercial entities subject to two conditions. Firstly, that particular province does not have a private sector data privacy legislation, or secondly, if such legislation exists, it has not been declared *substantially similar* to the PIPEDA.[221] Elder submits that for a provincial private sector legislation to be applicable in place of the federal legislation, 'each piece of provincial privacy legislation is examined against the federal law and the 10 privacy principles it embodies.'[222] Such provincial legislation is only applicable in place of the PIPEDA when it is pronounced *substantially similar* to the PIPEDA by the Governor in Council.[223] PIPEDA also applies to inter-provincial (out-of-province) and international data collection, use and disclosure.[224]

A vexed issue with regard to the geographical application of the PIPEDA is its extra-territorial scope. This is important because of the cross-border flow of personal information. In certain circumstances, personal information may be transferred to an organisation (which does not have a place of business or connection with Canada) outside Canada. In this regard, it has been argued that the PIPEDA is not a long-arm statute.[225] It strictly applies to organisations 'carrying on business in Canada'[226] (i.e. with a place of business or employees in Canada). In certain exceptional cases, however, its scope may also extend to cross-border transactions.[227] In *Lawson v Accusearch Inc,* [228] the Federal

---

220 Office of the Privacy Commissioner of Canada (n 84 above).

221 PIPEDA, sec 26 (2)(b) As of March 2015, only the Alberta's Personal Information Protection Act; British Columbia's Personal Information Act and Quebec's An Act Respecting the Protection of Personal Information in the Private Sector have been declared substantially similar. Some health sector privacy legislation have also been declared substantially similar to the PIPEDA. They are: Ontario - Personal Health Information Protection Act; New Brunswick - Personal Health Information Privacy and Access Act; Newfoundland and Labrador's - Personal Health Information Act; see Office of the Privacy Commissioner of Canada (n 91 above). It must be pointed out that even in these provinces, the PIPEDA continues to apply to federally regulated private enterprises such as telecoms, banking and transport as well as interprovincial and international transactions. PIPEDA also applies in health sectors of provinces without health sector law that are substantially similar. The requirement of *substantial similarity* was challenged by Quebec in 2003. Quebec contends that this provision is an intrusion into provincial jurisdiction and as such, constitutes a dangerous precedent. The matter is still before the SCC as there is no evidence that a decision has, yet, been reach. Nevertheless, Nisker argues that this act of the Canadian federal government is consistent with the Constitution and as such, the action by Quebec is most likely going to be fail. See J Nisker 'PIPEDA: A Constitutional analysis' (2006) 85 *The Canadian Bar Review* 317-342.

222 Elder (n 12 above) 42, see also McWilliam (n 40 above).

223 Elder (n 12 above) 42.

224 Piper (n 15 above) 266; London (n 7 above) 274.

225 A Siegel *et al* 'Survey of privacy law developments in 2009: United States, Canada, and the European Union' (2009) 65(1) *The Business Lawyer* 296.

226 Seigel (n 225 above) 296.

227 Seigel (n 225 above) 296,

228 (2007) FC 125 (Can.).

Court of Canada held that the Office of the Privacy Commissioner has a broad mandate to investigate entities that do not have infrastructure in Canada, but are processing Canadian's personal information.[229] It was further held that the Privacy Commissioner can investigate both foreign entities in possession of Canadians personal data and the Canadian sources themselves, insofar as there is a reasonable and substantial connection between the entity (or action complained of) and Canada.[230] This can therefore be said to be an extra-territorial reach of the PIPEDA which relies on a test called 'real and substantial connection to Canada' first propounded by the SCC in 1995.[231] Bennett *et al* also point out that the extra-territorial reach of the Act is expressed within the Act.[232]

The PIPEDA does not apply to: government institutions covered by the Privacy Act; any individual that collects, uses or discloses personal information for strictly personal or domestic purposes; and any organisation that collects uses or discloses personal data for journalistic, artistic and literary purpose.[233] Though not mentioned in the Act, Section 4.1.3 of the schedule refers to third party processing of personal data. Elder argues that 'such third party processors are not generally seen as being governed directly by the legislation, but rather by contract with responsible "organization", which is legally accountable for compliance.'[234]

d. Fair information principles (FIPs)

The PIPEDA benefitted immensely from the OECD Guidelines with respect to the FIPs.[235] It establishes ten FIPs which, according to Spaeth, 'represent the operative core of

---

229 The Company in question has no branch in Canada but was operating through a "dot.com" website. See also *Alteen v. Informix Corp* (1998) 164 Nfdl. 301 cited in Spaeth (n 211 above) 39.

230 (n 228 above); Siegel (n 232 above).

231 See CJ Bennett *et al* 'Real and substantial connections: Enforcing Canadian privacy laws against American social networking companies' (2014) 23(1) *Journal of Library and Information Science* 55. See also Office of the Privacy Commissioner of Canada *The case for reforming the Personal Information Protection and Electronic Documents Act* https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp (accessed 1 November 2015).

232 PIPEDA, sec 4.1.3 of the 1st Schedule. See also Bennett (n 231 above) 54 according to the scholar '[t]his provision in PIPEDA applies if the 'third party' is outside Canada, regardless of whether the organisation resides in a jurisdiction with equivalent privacy protection law.'

233 PIPEDA, sec 2.

234 Elder (n 12 above) 43.

235 PIPEDA incorporates principles outlined in the OECD Guidelines. See McWilliam (n 40 above). The OECD Guidelines is based on eight data privacy principles. They are limitation of collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. See also Spaeth (n 218 above) 30. See also L Austin 'Is consent the foundation of fair information practices? Canada's experience under PIPEDA' (2006) 56 *University of Toronto Law Journal* 194.

PIPEDA'.[236] In a unique style, the FIPs are not contained within the Act, rather they are in the schedule of the law.[237] That notwithstanding, section 5 provides that every organisation shall comply with the obligations set out in schedule one.[238] Schedule one contains the FIPs. The question then is whether this section requires a mandatory compliance with the principles provided in the schedule. It is the view of this researcher that there is nothing in the section or the law that suggests otherwise. The law makes copious references to the FIPs which depict their importance. Also, the word 'shall' as used in the section generally implies a mandatory obligation as against 'may' which is of a discretionary in nature. Thus, every organisation that falls within the scope of the PIPEDA must comply with the principles in the schedule.

Concerning the substantive principles, accountability comes first.[239] This principle holds an organisation responsible for personal information under its control. An organisation, in fulfilment of this principle, must designate an individual(s) (or a delegate to act on his/her behalf) who is accountable for the FIPs.[240] Assigning an individual does not relieve the organisation of the obligation to comply with the duties in the schedule.[241] This principle also holds an organisation responsible for the information transferred to a third party for processing.[242] Thus, the organisation must 'use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.'[243] Another dimension of accountability is that it obligates an organisation to implement policies and practices to give effect to the FIPs.[244]

The second principle is the principle of identifying purposes.[245] In terms of the Act, the purposes for which personal information is collected must be identified by the organisation at or before the time of collection.[246] The organisation must also document such purposes

---

236 Spaeth (n 211 above) 33.
237 See PIPEDA, Schedule 1 of the Law, based on principles set out in Canadian Standard Association (CSA) Model Code; all other provincial legislation do not adopt this approach. They all follow the traditional prescriptive format. Elder (n 12 above) 47.
238 However, subject to secs 6 to 9.
239 PIPEDA, sec 4.1 of the schedule
240 PIPEDA, 4.1.1 and 4.1.2 of the schedule; this also includes sufficient training of the designated official. See PIPEDA Report of Findings #2014-009 https://www.priv.gc.ca/cf-dc/2014/2014_009_0210_e.asp (accessed 1 November 2015).
241 PIPEDA, sec 6.
242 PIPEDA, sec 4.1.3 of the 1st schedule.
243 PIPEDA, sec 4.1.3 of the 1st schedule.
244 PIPEDA, sec 4.1.4 of the 1st schedule, eg of such policies and practices are stated in the sec.
245 PIPEDA, sec 4.2 of the 1st schedule.
246 See the Federal Court of Appeal's decision in *Englander* (n 207 above) 387.

for the sake of complying with the openness and individual access principles.[247] This principle is also linked to the limiting-collection principle in that, identifying the purpose for which information is collected enables organisations to determine the minimum information needed to fulfil such purpose and limits itself to such minimum information.[248] Furthermore, when the personal information is to be used for a purpose other than that identified, the new purpose must be identified before use.[249] Consent must also be sought from the individual unless the new purpose is required by law.[250]

Consent is the third principle and it is the primary requirement that legalises collection, use and disclosure of personal data in all data privacy laws.[251] In terms of the PIPEDA, '[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.'[252] Consent for use or disclosure must be sought, except in exceptional circumstance, at the time of collection and use.[253] The Act provides for knowledge and consent as it envisages a situation where there may be knowledge without consent. However, the individual must be informed, in a manner that he/she reasonably understands, of how the information will be used for the purpose of exercising meaningful consent.[254] Consent must be sought for collection, subsequent use or disclosure of personal information.[255] For meaningful consent, an organisation must not require an individual to consent to the collection, use or disclosure as a condition for the supply of a product and service over and above what is required to fulfil the explicitly specified and legitimate purposes.[256] The form of consent sought by the organisation may vary depending on the circumstances and sensitivity of the information.[257] Reasonable

247 PIPEDA, sec 4.2.1 of the 1st schedule.
248 PIPEDA, sec 4.2.2 of the 1st schedule, the identifying purpose principle is also linked to limiting use, disclosure, and retention principle (clause 4,5), 4.2.6.
249 PIPEDA, sec 4.2.4 of the 1st schedule. See also Cockfield (n 30 above) 335.
250 PIPEDA, sec 4.2.4 of the 1st schedule.
251 See eg, art 7(a) of the EU Directive.
252 PIPEDA, sec 4.3 of the 1st schedule.; the note in the sec gives eg of instances where information may be collected, used or disclosed without knowledge and consent and it include legal, medical and security reasons; detection and prevention of fraud or for law enforcement.
253 PIPEDA, sec 4.3.1 of the 1st schedule.
254 PIPEDA, sec 4.3.2 of the 1st schedule.; the Quebec private sector law requires that consent for the use or disclosure of personal information must be 'manifest, free, and enlightened' and it must also be given for specific purposes.
255 PIPEDA, sec 4.3.2 of the 1st schedule.
256 PIPEDA, sec 4.3.3 of the 1st schedule.
257 PIPEDA, sec 4.3.4 of the schedule; see also sec 4.3.6.

expectations of the individual are also relevant in obtaining consent.[258] The Act outlines several ways consent may be given by an individual[259] and provides that consent may be withdrawn at any time by the individual subject to legal, contractual restriction and notice.

The fourth principle is on limiting collection and it simply limits organisations in their collection of information to that which is necessary for the identified purpose.[260] This principle is for the purpose of ensuring fair and lawful collection so as to ensure organisations gather personal information lawfully devoid of deceit.[261] Thus, consent for collection must not be obtained through deception or fraud.[262] This principle is closely related to the identifying-purpose and consent principles considered above.[263] Principle five limits use, disclosure and retention of personal information. It is provided that personal information shall not be used or disclosed for other purposes outside that for which it was collected, except with consent or as required by the law.[264] It is linked to the other principles,[265] but its novelty is in providing for rules on retention. Principle five requires that '[p]ersonal information shall be retained only as long as necessary for the fulfilment of those purposes.'[266] Furthermore, organisations should develop guidelines and implement procedures with respect to retention of information, which should include minimum or maximum retention periods.[267] An obligation to delete personal information no longer required to fulfil the identified purpose is placed on the organisation.[268]

The sixth principle is on accuracy and it requires personal information to be accurate, complete and up-to-date for the identified purpose.[269] The extent of accuracy, completeness and up-to-date nature of personal information shall depend on the use of the

---

258 PIPEDA, sec 4.3.5 of the schedule. An individual giving consent to a bank will reasonably expect that the bank will, in addition to using the information, transfer it to the banking regulatory body. However, all depends on the circumstance.

259 PIPEDA, sec 4.3.7 of the 1st schedule.

260 PIPEDA, sec 4.4 of the 1st schedule.

261 PIPEDA, sec 4.4.2 of the 1st schedule.

262 PIPEDA, sec 4.4.2 of the 1st schedule.

263 PIPEDA, sec 4.4.3 of the 1st schedule.

264 PIPEDA, sec 4.5 of the 1st schedule.

265 PIPEDA, sec 4.5.4 of the 1st schedule especially consent, identifying purpose, and individual access principles.

266 PIPEDA, sec 4.5.3 of the schedule. The exception to this principle is contained in sec 8(8) which provides 'an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this part that they may have.

267 PIPEDA, sec 4.5.3 of the 1st schedule.

268 PIPEDA, sec 4.5.3 of the 1st schedule.

269 PIPEDA, sec 4.6 of the 1st schedule.

information, taking into account the individual's interest.[270] This principle is controversial as organisations may have to collect more personal data to keep information updated.[271] Nevertheless, such collection must be in line with the identified purpose. It is also provided that the routine updating of personal information is prohibited unless such a process is necessary to fulfil the identified purpose.[272] Spaeth therefore argues that the Act contradicts itself in this regard.[273] It is submitted that there is no contradiction as routine updating is allowed to fulfil the identified purpose so as to ensure accuracy. McClennan and Schick point out that 'PIPEDA presents organizations collecting information with a potential legal catch-22 because such organizations may have to go back to collecting information from the data subject not for identified purpose as at the time of original collection, but solely to comply with this law.'[274]

Principle seven stipulates that '[p]ersonal information shall be protected by security safeguards appropriate to the sensitivity of the information.'[275] Such security safeguards shall protect personal data against things such as loss, theft, unauthorised access and disclosure.[276] The Act recommends several methods of protection which include adoption of physical, organisational and technological measures.[277] The eighth principle is the openness principle and it provides that organisations shall make readily available specific information about their policies and practices on the management of personal information.[278]

Principle nine is directly related to the openness principle. It requires that individuals should, upon request, be informed and given access to their personal information.[279] Such individual should be able to challenge the accuracy of information and have it rectified. However, section 9(1) provides that an organisation should not give access if doing so will reveal personal information about a third party.[280] Finally, principle ten is on challenging

---

270 PIPEDA, sec 4.6.1 of the 1st schedule.
271 McClennan & Schick (n 29 above) 689.
272 PIPEDA, sec 4.6.2 of the 1st schedule. See also Spaeth (n 211 above) 36.
273 Spaeth (n 217 above) 36.
274 Mclennan & Schick (n 29 above) 689.
275 PIPEDA, sec 4.7 of the 1st schedule.
276 PIPEDA, sec 4.7.1 of the 1st schedule.
277 PIPEDA, sec 4.7.3 of the 1st schedule.
278 PIPEDA, sec 4.8.1 of the 1st schedule.
279 PIPEDA, sec 4.9 of the 1st schedule.
280 However, if personal information about a third party is severable, then access shall be granted. Sec 9 (1). Also, if the third party consents, access will be granted. See 9(2). There are also several well defined circumstances when access may be refused in sec 9(3).

compliance. It flows from the openness principle as an individual is granted the right to challenge compliance with all the above principles.[281] Upon challenge, an organisation shall investigate all complaints and if it is justified, such organisation must take appropriate measure including amending its policies.[282] This principle also highlights the crucial function of the designated privacy officer established by principle one.

The OECD Guidelines archetypes do not expressly provide for the fair and lawful processing of personal data as an independent principle. It is, however, contained in the various principles discussed above.[283] The Act also does not set out particular provisions for the purpose of protecting sensitive personal data.[284] This is, however, impliedly provided for in many of the principles.

e. Rights of individuals and duties of organisations

Unlike many other data privacy laws, the PIPEDA does not explicitly spell out the rights of individuals and duties of organisations. Most of these rights and duties are elaborately contained in the FIPs. Privacy advocates may criticise this approach. It is, however, submitted that the approach may be justified on the grounds that it eliminates unnecessary duplications which could make the law cumbersome and unnecessarily repetitive.

f. Exemptions and qualifications

The PIPEDA provides for instances where an organisation may be exempted from the requirement of consent when collecting, using or disclosing personal data. Thus, based on section 7(1), an organisation may collect personal information without knowledge and consent of the individual if the collection is in the interest of the individual and consent cannot be timely obtained. Other grounds for collection without knowledge and consent are: if such collection with knowledge and consent would compromise the availability or accuracy of the information and the collection is reasonable for purposes of investigating a

281 PIPEDA, sec 4.10 of the 1st schedule.
282 PIPEDA, sec 4.10.4 of the 1st schedule.
283 See eg, principle 4.2 of the 1st schedule.
284 Unlike the Quebec Act which provides special rules on handling of sensitive personal information. See (n 219 above) secs 70-79.

breach of agreement or law; for journalistic, artistic or literary purpose; if the information is publicly available; or collection is for making lawful disclosures.[285]

Similarly, an organisation may use personal information without knowledge and consent if: the organisation becomes aware of information that it has reasonable ground to believe could be useful for investigation purposes; the information is used for emergency situation being an emergency that threatens the life, health or security of an individual; the information is used for statistical, scholarly and research purposes;[286] or if the information is publicly available.[287]Also, an organisation may use personal information for purposes other than those for which it was collected in the above circumstances.[288]

Disclosure without knowledge and consent appears to have been granted greater exemptions under the PIPEDA. It includes a broad range of instances - disclosures made to an advocate or solicitor representing an organisation; for purposes of collecting debt owed by the individual to the organisation. Other exemptions for disclosure without knowledge and consent include: for compliance with a subpoena or warrant or order of court and disclosure to an agency of government that has the lawful authority to obtain same. Similarly, an organisation may also disclose personal information for purposes other than those for which it was collected in the above circumstance.[289] It is submitted that all instances of disclosures provided for are carefully tailored for lawful purposes and none appear to give the organisation too much discretion with respect to disclosures.

g. Transborder data flow regime under the PIPEDA

The PIPEDA does not restrict the transborder flow of personal information.[290] Rather, it provides an innovative approach to data privacy protection in interprovincial and international transfers of personal data. It is provided in the schedule of the PIPEDA that '[a]n organization is responsible for personal information in its possession or custody'. This includes information being transferred to a third party (whether international or

285 PIPEDA, sec 7(1).

286 In this case, the innovative approach of the PIPEDA is that it does not merely exempt use of personal information for scholarly, research statistical purpose with a blanket provision. It also provides for a confidentiality principle in that such use must be 'in a manner that will ensure its confidentiality' also, it must be impracticable to obtain consent and the organization must inform the commissioner of the use before the information is used. See London (n 7 above) 278.

287 PIPEDA, sec 7(2).

288 PIPEDA, sec 7(4).

289 PIPEDA, sec 7(5).

290 McClennan & Schick (n 29 above) 657 & 686; Keith (n 219 above).

interprovincial) for processing.[291] The Act also recommends means for protecting such personal information. It provides that 'the organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.'[292] The Act effectively establishes an 'agency concept' with regard to transborder data transfers.[293] Bennett *et al* contend that section 4.1.3 "applies if the 'third party' is outside Canada, regardless of whether the organisation resides in a jurisdiction with equivalent privacy protection law."[294] They further point out that the approach 'of requiring specific contractual or other guarantees, is often held up as an alternative to the international data flow restriction inherent within the EU Directive'.[295] It must be pointed out that certain provinces, however have an adequacy requirement for transborder transfers of personal data like the EU style.[296]

4.4.2.4. A critique of the PIPEDA: Protecting human rights or enhancing commerce?

The PIPEDA has far reaching provisions protecting the data privacy rights of individuals. It extensively provides for FIPs in a clear and coherent manner. Unlike the Privacy Act, there are fewer exceptions under the PIPEDA.[297] Nevertheless, the PIPEDA, like any good law, has also been the subject to criticism. The style of making the FIPs an annexure in the law has provoked comments from critics. It has been stated to be a 'badly fitting hand me down' and a 'Frankenstein monster'.[298] In this respect, Keith argues that the law which started out as a voluntary model code has been effectively stapled to the back of an Act of Parliament and made compliance mandatory rather than voluntary.[299] It is also opined that enforcement under the PIPEDA is generally lax.[300] Furthermore, the Act distinguishes between the stages of data processing (collection, use and disclosure) which makes its provisions a bit monotonous and repetitive. It is the view of this researcher that all the

---

291 PIPEDA, sec 4.1.3 of the 1st schedule. Generally, the PIPEDA does not distinguish between domestic and international data flow and a 'data transfer' is considered as 'use' of data by an organisation. See Office of the Privacy Commissioner of Canada, 'Guidelines for Processing Personal Data across Borders' (2009), http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf (accessed 1 November 2015) 5. See also C Kuner *Transborder data flows and data privacy law* (2013) 11.

292 PIPEDA, sec 4.1.3 of schedule 1.

293 As extrapolated by Keith (n 219 above); McClennan & Schick (n 29 above) 686 fn 80.

294 Bennett (n 231 above) 55.

295 Bennett (n 231 above) 55.

296 British Columbia has an 'adequacy' requirement in its private sector privacy law. See Geist & Homsi (n 25 above) 277.

297 McClennan & Schick (n 29 above) 686.

298 Keith (n 219 above).

299 Keith (n 219 above).

300 Keith (n 219 above).

various stages of data processing brings about similar risks as a consequence, there is no need to distinguish between them. Moreover, Roos points out, quite rightly, that the trend among recent data privacy legislation is no longer to distinguish between these stages but to use a generic term 'processing' which is broad enough to cover all the stages.[301]

The above notwithstanding, the issue that provokes debates with regard to the PIPEDA is the controversial issue of whether it is a law that protects human rights or one that enhances commerce. This issue is crucial given the growing contention that a data privacy instrument with pure human rights objectives is more likely to be effective for guaranteeing the freedom and autonomy of individuals.[302] Both a commercial and a human rights agenda can, arguably, be inferred from the provisions of the law. Particularly, section 3 which contains the purpose of the law seems to encompass both agendas (i.e. human rights and commerce).

The title of the law shows more of a commercially driven motive as it expressly claims to 'support and promote electronic commerce' by protecting personal information. Most privacy advocates are also of the view that the PIPEDA is 'unquestionably a commercially-driven piece of legislation and, from their perspectives, most of its weaknesses stem from this fact.'[303] Flaherty for example, unequivocally argues that the PIPEDA was certainly about 'protection for business'[304] even though the drafting process drew heavily on the work of experts who preferred a human rights approach.[305] Similarly, Piper contends that the Act was not passed as substantive privacy protection legislation. Instead, its purpose is to facilitate e-commerce by reassuring Canadians that their personal information may be protected.[306]

There are a number of reason why the Canadian government opted for a commercially driven approach, the most important of which is that 'Industry Canada saw data privacy protection as a key plank into its e-commerce strategy' and the need to satisfy the business community which preferred self-regulation.[307] As noted above,[308] one of the driving forces

---

301 A Roos 'Personal data protection in New Zealand: Lessons for South Africa (2008) 4 *Potchefstroom Electronic Law Journal* 79.

302 See generally PA Bernal *Internet privacy rights: rights to protect autonomy* (2014).

303 This is based on an interview conducted by Berzin with Bennett and Flaherty. See Berzins (n 187 above) 624.

304 Berzins (n 187 above) 624.

305 Berzins (n 187 above) 624.

306 Piper (n 15 above)262.

307 Naturally like the US approach. Berzins (n 184 above) 625.

behind the enactment of the PIPEDA is the EU Directive's adequacy requirement.[309] Bennett observes that the enactment of the Directive 'meant that no jurisdiction in Canada (save Quebec) could plausibly claim an "adequate level of protection" and therefore process personal data transmitted from Europe.'[310] This commercial emphasis, according to the author, 'explains why Industry Canada[311] always spearheaded initiatives towards the enactment of the PIPEDA.'[312] This further justifies any argument for its commercial agenda. Thus, it is submitted that though the PIPEDA has a high level regard for human rights to data privacy, its commercial agenda is the primary driving force.

Although the PIPEDA may be said to be commercially driven, the Office of the Privacy Commissioner and the Courts have consistently ensured that there is a high level of compliance with the FIPs. These institutions have, arguably, applied a human rights-based approach to a commercially driven piece of legislation, and in many cases, data privacy rights prevail over the interests of business entities.

4.4.2.5. Health sector

Canada is one of the few jurisdictions in the world with a dedicated framework for protection of personal information in the health sector. This, however, exists only in certain provinces as the PIPEDA largely protects personal health information at the federal level.[313] In provinces that do not have a dedicated structure for protection of personal health information, their public and private sector privacy legislation is applicable. Though, it was stated at the onset that this chapter only considers legislation at the federal

---

308 In discussing historical perspective of the PIPEDA.

309 Piper (n 15 above) 262.

310 CJ Bennett 'The privacy commissioner of Canada: Multiple roles, diverse expectations and structural dilemmas' (2003) 46 *Canadian Public Administration* 221.

311 Industry Canada is a Canadian federal government agency whose primary mandate 'is to help make Canadian industry more productive and competitive in the global economy, thus improving the economic and social well-being of Canadians.' See Industry Canada 'About us' http://www.ic.gc.ca/eic/site/icgc.nsf/eng/h_00007.html (accessed 1 November 2015).

312 Bennett (n 310 above) 221.

313 Alberta: Health Information Act, RSA 2000, c H05; British Columbia: E-Health (Personal Health Information Access and Protection of Privacy) Act, SBC 2008, c 38; Manitoba: Personal Health Information Act, CCSM, c P33.5, New Brunswick: Personal Health Information Privacy and Access Act, SNB. c P-7.05.; Newfoundland and Labrador: Personal Health Information Act, SNL. 2008, c P-7.01.; Nova Scotia: Personal Health Information Act, SNS. 2010, c 41.; Ontario: Personal Health Information Protection Act, 2004, SO 2004, c 3.; Quebec: An Act respecting access to documents held by public bodies and the protection of personal information, RSQ., c A-21.; An Act respecting the protection of personal information in the Private sector, RSQ., c P-39.1.; Saskatchewan: Health Information Protection Act, SS. 1999, c H-0.021. It must be stated that the Ontario's, New Brunswick and Newfoundland and Labrador's Health information Acts have been declared 'substantially similar. Office of the Privacy Commissioner of Canada (n 84 above).

level, it is the view of the researcher that vital insights can be derived from this system.[314] This is more so in a country like Nigeria that is in the process of developing an Electronic Health Record (EHR) system in the health sector.[315]Commentators have also acknowledged the importance of sectoral legislation in the scheme of personal data protection.[316] For the purpose of emphasis, sectoral legislation, especially in a specialised and technical area like the health sector, will give room for a coherent policy that focuses on the peculiar challenges of processing of personal health information.[317]

a. Purpose of the law

The health sector law is usually to regulate the collection, use, disclosure and retention of personal health information. For example, Nova Scotia Personal Health Information Act ('Personal Health Information Act')[318] provides that its purpose is 'to govern the collection, use, disclosure, retention, disposal and destruction of personal health information in a manner that recognises both the right of individuals to protect their personal health information and the need of custodians to collect, use and disclose personal

---

314 For more on the need for the protection of personal health information in Nigeria with special focus on mobile health, see OO 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' unpublished LLM thesis, Dalhousie University, 2015. In addition, for more elaborate discussion of the need for an elaborate protection of patient's records, see AO Adesina *et al* 'Ensuring the security and privacy of information in mobile health-care communication systems' (2011) 107 (9/10) *South African Journal of Science* 1-7.

315 There are calls for Nigeria to adopt the Electronic Health Record (EHR) system for the whole country because of its potential benefits. JS Pantuvo *et al* 'Towards Implementing a Nationwide Electronic Health Record System in Nigeria' (2011) 3 *International Journal of Healthcare Delivery Reform Initiatives* 39-55.

316 DW Schartum 'Designing and formulating data protection laws' (2010) 18 *International Journal of Law and Information Technology* 1-27; see also Bennett & Raab (n 10 above) 131 and DH Flaherty *Protecting privacy in surveillance societies* (1989) 404-405.

317 Eg, the US passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a specialised legislation for protection of personal health information in the health sectors so as to prevent discrimination or denial of employment based on medical information. This Act has however been amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) which places obligation of data breach notification on entities within its scope. The new legislation is said to be the "first significant national reporting statute" and strengthens enforcement regime in the health sector. See KJ Nahra, A new HIPAA era emerges, privacy in focus (2009) 3-4, available at http://www.escaladeit.com/sites/default/files/A_New_HIPAA_Era_Emerges.pdf (accessed 1 November 2015).

318 Nova Scotia Personal Health Information Act Chapter 41 of the Acts of 2010 available at http://nslegislature.ca/legc/bills/61st_2nd/3rd_read/b089.htm (accessed 1 November 2015). I will be focusing on this law for the purpose of discussing regulation of health sector processing of personal data because it is the most recent personal health privacy law in Canada as it received royal assent only in December 2010. This means it will, arguably, contain provisions which tackle emerging challenges to personal health information in a more modern form.

health information to provide, support and manage health care.'[319] Like PIPEDA, the Act also advocates a balancing approach.

b. Jurisdiction and application of the law

Section 5 provides that the Act applies to the collection[320] of personal health information by a custodian; the use[321] or disclosure[322] of same (personal health information) by a custodian or a person who is not a custodian and to whom a custodian discloses the information. The Act also applies to the collection, use or disclosure of a health-card number.[323] The Act defines personal health information in a similar way as the PIPEDA. It provides that personal health information is information that identifies an individual, whether living or deceased, and in both recorded and unrecorded forms.[324] Furthermore, such information must relate to either: the physical health of the individual or health history of the individual's family; or application, assessment, eligibility and provision of health care to the individual; or to payments or eligibility for health care of an individual; or the donation of body part or bodily substance by an individual or information derived from testing or examination of such. In addition, personal health information could include an individual's registration information such as the individual's health-card number; or information which identifies an individual's substitute decision-maker.[325]

A custodian is defined as 'an individual or organization … who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties.'[326] Examples of custodians as provided by the Act include a regulated health professional, the Minister of health promotion and protection, a district health authority, a pharmacy and the Canadian blood services. The definition shows that the Act is not only applicable to medical or health care practitioners, but any person who has control (direct or indirect) of health records. The Act has a broad scope and even covers 'a person who is not a custodian and to whom a custodian discloses the

319 Personal Health Information Act, sec 2.
320 Collection means 'to gather, acquire, receive, gain access to or obtain the information by any means from any source.' Personal Health Information Act, sec 3 (c).
321 Use 'means to handle or deal with the information, but does not include to disclose the information.' Personal Health Information Act, sec 3(a)(b).
322 Disclosure 'means to make the information available or to release it to another custodian or to another person, but does not include to use the information' Personal Health Information Act, sec 3(h).
323 Personal Health Information Act, sec 5.
324 Personal Health Information Act, sec 5.
325 Personal Health Information Act, sec 3(r).
326 Personal Health Information Act, sec 3(f).

information'.[327] This shows the degree of sensitivity the processing of personal health information entails.

Health sector data privacy laws usually do not apply to: statistical, aggregate or de-identified health information; personal health information about an individual one hundred and fifty (150) years after the record was created or fifty (50) years after the death of the individuals whichever is earlier;[328] and solicitor-client privileged communication.[329] The law is also not applicable, unless specifically provided otherwise, to individuals or organisations that collect, use or disclose personal health information for purposes other than health care and the planning and management of the health care systems.[330] This includes the processing of personal information by employers, insurance company and regulated health-professional bodies. It is submitted that this exclusion is unwarranted as the collection and use of personal information by this category of persons also present similar risks to individuals. Nevertheless, since persons in this category are not strictly custodians as narrowly defined by the Act, they will fall within the scope of other data privacy laws like the PIPEDA.

c. Fair Information Principles

Like the Privacy Act, the FIPS in the health sector law are not outlined in a section of the law. Unlike in the PIPEDA, they are contained in the substantive provisions of the Act. The strict distinction between collection, use and disclosure of personal information is also maintained by the Act.

Section 11 provides that a custodian shall not collect, use or disclose personal health information about an individual unless there is *consent* and the collection, use or disclosure is 'reasonably necessary for a lawful purpose' or the collection, use or disclosure is permitted or required by the Act.[331] Like the PIPEDA, knowledge is required in addition to consent.[332] The Act also makes provisions for consent by a substitute decision-maker if the

327 Personal Health Information Act, sec 5.
328 Personal Health Information Act, sec 5(2).
329 Personal Health Information Act, sec 5(3).
330 Personal Health Information Act, sec 6(1).
331 Personal Health Information Act, sec 11 (a)(b).
332 Personal Health Information Act, secs 12, 13, 15.

individual lacks the capacity to make a decision.[333] Such substitute decision-maker must be chosen from a list of persons contained in the Act.[334]

A custodian is prohibited from collecting, using or disclosing personal health information if other information will serve such purposes.[335] If otherwise, the collection, use, and disclosure of health information must be limited to the amount necessary to achieve the purpose of collection, use and disclosure.[336] Thus, the general rule seems to be that the collection of personal health information is prohibited except if there is no alternative. This provision also goes to show the high degree of sensitivity of personal health information.

It is also stated that a custodian is permitted to collect personal health information only for a lawful purpose related to his/her authority or if such collection is expressly authorised by the Act or any other law of Canada.[337] A custodian must also only collect personal health information directly from the individual except: if such individual authorises collection from another person; if the collection is from a substitute decision-maker; if the information is necessary for providing health care and it is not reasonably possible to collect directly from the individual; or if collection from the individual will prejudice his/her safety etc.[338]

Personal health information can only be used for the purposes for which the information was collected and for functions reasonably necessary for carrying out that purpose or a purpose the law permits; or for educating agents to provide health care.[339]A custodian may only disclose personal health information about an individual to another custodian if the disclosure is reasonably necessary for the provision of health care to the individual.[340] A custodian must 'securely destroy' erase or de-identify personal health information that is no longer required to fulfil the identified purpose of retention.[341] Personal health information can also be used and disclosed by a custodian for research purposes. Such

333 Personal Health Information Act, sec 21(1)
334 Personal Health Information Act, sec 21(2).
335 Personal Health Information Act, sec 24.
336 Personal Health Information Act, sec 25.
337 Personal Health Information Act, sec 30.
338 Personal Health Information Act, sec 31.
339 Personal Health Information Act, sec 33.
340 Personal Health Information Act, sec 36.
341 Personal Health Information Act, sec 49.

disclosure must, however, be 'limited to the minimum amount of information necessary to accomplish the research purpose.'[342]

d. Rights of individuals and duties of custodians

Outside the above general principles of data privacy, specific obligations are placed on the custodian to protect personal health information. This further depicts the value and sensitivity of personal health information. A custodian is required to protect the confidentiality and privacy of information under his/her custody or control.[343] He/she must also implement, maintain and comply with the information practices under the Act that are reasonable in the circumstances.[344] Very importantly, with respect to protection of personal health information in the computer age, is section 65 which requires a custodian who maintains an electronic information system to implement any additional safeguards for such information required by the regulation.[345] A custodian must also designate one or more individuals to act on his/her behalf to facilitate compliance with the Act.[346] He/she shall make available to the public a written statement that provides a general description of his/her information practices, the contact person, the means of access to information or the means to request correction of personal information in his/her custody and the complaints procedure.[347] A custodian has a duty of data breach notification.[348]

Individuals have been further granted certain rights to enhance control of their personal health data. An individual has a right of access to a record of his/her personal information in the custody or control of a custodian.[349] Where such access is granted and the individual believes that the record is not accurate, complete or up-to-date, the individual has a right to request a correction in writing or orally.[350] Similarly, where an individual believes that a custodian has contravened the Act, or has refused to grant access or to make a correction, he/she may request a review.[351]

---

342 Personal Health Information Act, sec 54.
343 Personal Health Information Act, sec 61.
344 Personal Health Information Act, sec 62.
345 Personal Health Information Act, sec 66.
346 Personal Health Information Act, sec 67.
347 Personal Health Information Act, sec 68.
348 Personal Health Information Act, sec 69 & 70.
349 Personal Health Information Act, sec 71.
350 Personal Health Information Act, sec 85.
351 Personal Health Information Act, sec 91.

4.4.2.6. A critique of the health sector data privacy regime[352]

There is much to learn from this approach of setting out *sui generis* rules on processing of personal health information in Canada. Because of the delicate nature of personal health information, more elaborate protection is generally granted and more duties are placed on custodians in regard to the handling of personal information. Certain observations can be made with regard to this regime which is worthy of note.

Firstly, there are specific provisions which are specially tailored for health matters, for example the inclusion of a body part or bodily substances of an individual as part of the definition of personal health information.[353] Secondly, there is a stiffer consent requirement in health information laws than in other general data privacy laws. Thirdly, consent powers are granted to substitute decision-makers, as in many cases, the individual may not have the requisite capacity to grant or refuse consent due to health-related issues.[354] Fourthly, the provisions of this category of laws (health information laws) are more explicit so as to allow more certainty in the application of the law.[355] Nonetheless, like any data privacy law, there are quite a number of provisions that exempt custodians from the requirements of the law especially with respect to consent for use and disclosure of personal health information.[356] It must, however, be stated that most of these exemptions are *prima facie* justifiable.

4.5. An analysis of the oversight and enforcement structure of data privacy laws in Canada

It is not enough to have lofty laws on data privacy. [357] There must also be a complementary enforcement and oversight structure. Bennett and Raab observe that the existence of vigorous supervisory authorities is *sine qua non* to good privacy protection.[358] Accordingly, a lot of debate on the Canadian data privacy regime is centred on the oversight and enforcement institution. Canada has adopted a unique approach to oversight

352 For convenience, analysis in this part will focus on the Nova Scotia Personal Health Information Act for two reasons. First, most of the health sector laws in Canada contain essentially similar provisions and second, it is the most recent health sector law in Canada.
353 See Personal Health Information Act, Sec 3 (r).
354 Personal Health Information Act, sec 21 & 22.
355 Eg, sec 25 (2).
356 Eg, secs 35 &38.
357 Flaherty (n 315 above) 391.
358 Bennett & Raab (n 10 above) 133.

and enforcement of data privacy laws that has been applauded by some commentators.[359] This approach, however, has also been subject of much criticism.[360] Nova points out that data privacy law in Canada 'is enforced internally via a series of measures which allow for a mixture of self-help, access to the court system, and the assistance of a Canadian Privacy Commissioner.'[361] Based on this understanding, the court and the Privacy Commissioner are the key oversight and enforcement bodies of data privacy law. This description of Canadian oversight and enforcement institution may appear too simplistic as Bennett contends that:

> [t]he Office of the Privacy Commissioner [OPC] is the main, but not the only, agency responsible for the oversight of privacy protection policy. Day-to-day advice on the implementation of the Privacy Act is the responsibility of the Treasury Board, which also compiles and publishes the list of personal information banks. With respect to the PIPEDA, Industry Canada performs some wider policy functions, although there is tension with the OPC on the appropriate division of responsibilities. The Information and Privacy Branch of the Department of Justice gives day-today legal advice on the interpretation of both privacy and access-to-information statutes. The Privacy Act is also clear that primary responsibility for implementation rests with the "designated minister" or "head" of the government institution in question.[362]

The above, therefore, shows the obviously complicated structure of oversight and enforcement of data privacy laws in Canada. For the purpose of this analysis, however, only the Privacy Commissioner and the Courts will be considered. This is because of the international trend of designating enforcement and implementation responsibilities to these bodies.[363]

4.5.1. The Canadian Privacy Commissioner: Nature, functions and role

The Office of the Privacy Commissioner oversees the application of and compliance with Canada's two major data privacy laws.[364] In terms of both laws, the office is headed by the Privacy Commissioner who 'is independent of the Prime Minister's Cabinet and reports

---

359 EPIC & Privacy International (PI) 'Privacy and human rights report' http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Contents.html (accessed 1 November 2015).

360 Berzins (n 187 above).

361 Though the learned author was making reference to the PIPEDA only, I see application of these measures under the Privacy Act too. See also Nova (n 49 above) 782.

362 Bennett (n 310 above) 225.

363 See EU Directive, art 22 & 28.

364 McClennan & Schick (n 29 above) 683.

directly to the Canadian House of Commons and the Senate.'[365] The Privacy Commissioner is assisted by an Assistant Privacy Commissioner and other staff.[366] It is usually said that the Canadian data protection agency/authority (DPA) adopts an ombudsman model as the Privacy Commissioner is generally seen to be an Ombudsman. This model was 'consistent with Canadian constitutional norms, and was a fashionable solution'.[367] The need for this approach arose because of the necessity to give Canadians more effective protection of their personal data, unlike the US.[368] It is also a rejection of the 'overtly bureaucratic approach adopted by some European states.'[369] It is submitted that, to describe the Canadian Privacy Commissioner solely as an ombudsman is too simplistic and restrictive of his/her role.

Accordingly, Bennett and Raab maintain that irrespective of legislative powers, every Privacy Commissioner in Canada and every other jurisdiction in the world ought to perform seven key interrelated roles.[370] 'The Commissioner is an ombudsman for citizen complaints, an auditor of organisational practices, a consultant on new and existing information systems, an educator of the public, a policy adviser, a quasi-judge and a regulator of business.'[371] In a more recent publication, Bennett added one more role which is the role of an international ambassador.[372] These roles make the Privacy Commissioner 'a hybrid and difficult to classify according to any of the traditional conceptions of

---

365 McClennan & Schick (n 29 above) 683, Privacy Act, sec 53 provides for appointment of the Privacy Commissioner. The PIPEDA makes reference to the Privacy Act by providing that a Commissioner is Privacy Commissioner appointed under sec 53 of the Privacy Act. There are quite a number of issues on the requirement of independence of Privacy Commissioner which will not be considered in this chapter. However, for more on the requirements of independence of data privacy agencies, see G Greenleaf 'Independence of data privacy authorities (Part I): International standards' (2012) 28 *Computer Law & Security Review* 3-13; G Greenleaf 'Independence of data privacy authorities: International standards and Asia-Pacific experience' (2012) 23 *Computer Law & Security Review*; see also Bygrave (n 45 above) 170.

366 Privacy Act, secs 56, 57 & 58.

367 Especially because of the establishment of other ombudsmen for official languages and correctional investigations. See Bennett (n 1 above) 567.

368 Bennett (n 1 above) 566. Though Canada and the US have always regulated privacy in similar ways, the major difference is with respect to office of the privacy commissioner. See CJ Bennett & CD Raab 'The Adequacy of the European Union Data Protection Directive and the North American response' (1997) 13 *The Information Society: An International Journal* 247.

369 Bennett (n 1 above) 566.

370 Bennett & Raab (n 10 above) 109-114; see also Bennett (n 310 above) 236-237.

371 Bennett (n 310 above) 220; Bygrave mentions some of these role which are handling complaints, auditing, advisors. See Bygrave (n 38 above) 169.

372 C Bennett 'The role of a Privacy Commissioner and the qualifications of Daniel Therrien: What parliament should be asking' June 2014 available at http://www.colinbennett.ca/2014/06/the-role-of-a-privacy-commissioner-and-the-qualifications-of-daniel-therrien-what-parliament-should-be-asking/ (accessed 1 November 2015).

regulatory or oversight agencies.'[373] The roles, according to Bennett, 'may not be explicit in national legislation, and they obviously assume different weights in different contexts.'[374] The Commissioner needs to, however, consider how to perform each of these roles.[375] Analysis of the role of the Privacy Commissioner is therefore going to be carried out based on Bennett and Raab's elucidation above.

4.5.1.1. The Privacy Commissioner as an ombudsman

The first mission of the Office of Privacy Commissioner is 'to be an effective ombudsman's office, providing thorough and timely complaint investigations to ensure Canadians enjoy the rights set out in the Privacy Act.'[376] An ombudsman is an official normally appointed to investigate complaints against a company or organisation, especially a public authority.[377] This implies a non-confrontational and non-adversarial role.[378] Based on this understanding, it can be argued that the role of the Privacy Commissioner is effectively divided in stages as provided by two data privacy law. First is the receipt of a complaint against a government or private entity from an individual.[379] If satisfied that there is a reasonable complaint, a notice of the complaint is issued to the government establishment or company concerned. [380] The Commissioner shall thereafter investigate.[381] Finally, the Commissioner issues a report containing his/her findings.[382] The Ombudsman (and ultimately, the Privacy Commissioner's) role ends after the issuing of the report. All subsequent action lies with the courts as will be discussed shortly.

Although the law grants individuals an unfettered right to initiate complaints, in practice however, there is the implicit understanding that the Privacy Commissioner should be a last resort.[383] There are various avenues for resolving privacy issues especially in the private sector, such as a resolution by a designated individual (privacy officer) in an

373 Bennett (n 310 above) 220.
374 Bennett (n 310 above) 237.
375 Bennett (n 310 above) 237.
376 'The information technology landscape in Canada' http://www1.american.edu/carmel/sa0565a/leg_env.htm (accessed 1 November 2015). See also Bennett & Raab (n 10 above) 135.
377 *The concise oxford dictionary* (n 166 above).
378 Office of the Privacy Commissioner of Canada 'Presentation to E-Commerce and Privacy implementing the new law in the public and private sectors' February 21, 2000 https://www.priv.gc.ca/media/sp-d/02_05_a_000221_2_e.asp (accessed 1 November 2015).
379 PIPEDA, sec 11; Privacy Act, sec 29.
380 PIPEDA, sec 11(2) & (4); Privacy Act, sec 31.
381 PIPEDA, sec 11(2) &12; Privacy Act, sec 29 (3) and s 31.
382 PIPEDA, sec 13; Privacy Act, sec 35.
383 Bennett (n 310 above) 227.

organisation or through trade associations.[384] This is in order to enable the private sector to settle privacy issues without unnecessary expenses and publicity.[385] Resorting to the Privacy Commissioner only as a last resort seems to have been sanctioned by the PIPEDA.[386]

The power of an ombudsman (and the whole ombudsman structure) of the Commissioner has been commended in succinct words by the Commissioner's office. It was stated that:

> [t]he great advantage of this ombuds structure lies in the ability to audit and investigate conduct of government institutions without automatically importing the adversarial atmosphere that would arise if the Commissioner had specific powers of enforcement. The chief strengths in the ombuds role lie in effective research and negotiation with government institutions. As a last resort, and to be used only with clear justification, there is what we can call the power of embarrassment.[387]

The above quote highlights another important role of the Privacy Commissioner which will now be considered.

4.5.1.2. The Privacy Commissioner as an Auditor

It has been rightly observed that the complaints resolution (ombudsman role) of the Privacy Commissioners is reactive rather that proactive.[388] In many cases, the Commissioner only conducts investigations when complaints are received. Thus, the question remains whether the Commissioner could investigate without receiving a complaint? That is, should it be more proactive?[389] These investigations would be in the form of carrying out *audits* and *reviews* of privacy practices of governments and organisations before they actually infringe on individuals' data privacy rights. Indeed, this is a vital measure towards ensuring a high level of compliance with data privacy laws. Thus, Flaherty points out that the conducting of audits can be an effective way to implement the FIPs.[390] The Canadian data privacy laws, therefore, provide for instances where the powers of the Privacy Commissioner may be proactively activated based on suspicions of questionable data privacy practices.

---

384 Bennett (n 310 above) 227.
385 Bennett (n 310 above) 227.
386 PIPEDA, sec 12 (1) (a).
387 Office of the Privacy Commissioner of Canada (n 376 above).
388 Bennett (n 310 above) 228, Bennett & Raab (n 10 above) 135.
389 Bennett (n 310 above) 228.
390 Flaherty (n 316 above).

In terms of section 18 of the PIPEDA, the Commissioner may audit personal information management practices of an organisation upon a 'reasonable ground to believe' that the organisation contravenes certain provisions of the law.[391] Several powers are granted to the Commissioner to enable him carry out effective audits.[392] For example, section 37 of the Privacy Act provides that '[t]he Privacy Commissioner may, from time to time at the discretion of the Commissioner, carry out investigations in respect of personal information under the control of government institutions to ensure compliance with sections 4 to 8.' Similar powers are granted to the Commissioner to review the contents of an exempt bank under the Privacy Act.[393] The power of an audit (and a review) is so crucial that a dedicated branch in the Office of the Privacy Commissioner (*the privacy practices and review branch*) is set up for this.

It may be argued that a Privacy Impact Assessment (PIA) is a component of the audit role of the Privacy Commissioner.[394] This is because it has, over time, been understood to mean 'a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme.'[395] Like the auditing function, it is also proactive in nature. Nevertheless, Clarke contends that a PIA is different from the audit role 'because of its anticipatory, positive and risk management orientation'.[396] Thus, a PIA is anticipatory of the negative impact of a proposed project, unlike auditing which scrutinises existing data privacy practices of an organisation. Also, a PIA is usually initiated by a project manager under the guidance of the organisation's privacy officer.[397] The auditing function is largely a responsibility of the Privacy Commissioner. The requirement of a PIA is, however, mandatory for certain government agencies.[398]

---

391 PIPEDA, sec 18.

392 PIPEDA, sec 18 (1) such as summons and enforce appearance of persons, administer oaths, receive evidence, enter premises, converse in private with any person, examine or obtain copies of or extracts from records.

393 PIPEDA, sec 36.

394 On the contrary, Bayley and Bennett state that 'reviews (audits) are an effective part of PIA system in Canada and provide much additional value'. See RM Bayley & CJ Bennett 'Privacy impact assessments in Canada' in D Wright & P De Hert (eds) *Privacy impact assessment* (2012) 175.

395 R Clarke 'Privacy impact assessment: its origins and development' (2009) 25 *Computer Law & Security Review* 123.

396 Clarke (n 395 above), 130.

397 D Wright 'The state of the art in privacy impact assessment' (2012) 28 *Computer Law & Security Review* 56.

398 See Treasury Board Directive on Privacy Impact Assessment http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308 (accessed 1 November 2015).

4.5.1.3. The Privacy Commissioner as a consultant

The Privacy Commissioner is a consultant to both organisations and government entities for data privacy related issues on new and existing information systems.[399] His/her specialised skills and experience coupled with his/her numerous publications put the Privacy Commissioner in the best position to be consulted for data privacy related issues. For example, Stoddard points out that the Office of the Privacy Commissioner was consulted by the Treasury Board when developing the Policy on Privacy Protection 2014 to compliment the Privacy Act.[400]

4.5.1.4. The Privacy Commissioner as an educator

Another proactive role of the Privacy Commissioner under the law is 'to educate Canadians, to encourage knowledge and understanding of privacy.'[401] This is a vital role which involves promoting public awareness and understanding of privacy issues.[402] Unlike the Privacy Act, the PIPEDA provides for this role. Section 24 requires that the Commissioner shall develop and conduct programs to foster public understanding of the law.[403] He/she shall also undertake and publish research on data privacy issues.[404] As an extension of this role, the Commissioner performs an educational function by exposing privacy issues that need to be debated and discussed.[405] Thus, his/her educational function includes 'the articulation and advancement of the privacy interest that must be defended in a particular setting.'[406] This role is one of the outstanding features of the Canadian data privacy regime. The rich jurisprudence from the submissions, presentations and reports of the Privacy Commissioner in the Office of the Privacy Commissioner's website justifies this assertion.[407] The communications and strategic analysis department of the Office is making serious efforts in publications of news releases, conference speeches.[408] The Privacy Commissioners of the provinces are also making significant efforts in exposing

399 Bennett (n 310 above) 220.
400 Stoddart (n 33 above).
401 Office of the Privacy Commissioner of Canada (n 376 above).
402 Office of the Privacy Commissioner of Canada 'About the Office of the Privacy Commissioner' https://www.priv.gc.ca/au-ans/index_e.asp (accessed 1 November 2015). In fact, in the data privacy legislation of British Columbia, Alberta and Ontario, the Privacy Commissioner is expressly given the mandate to inform the public about their legislation.
403 PIPEDA, s 24 (a).
404 PIPEDA, sec 24(b).
405 Flaherty (n 93 above) 30.
406 Flaherty (n 93 above) 30.
407 https://www.priv.gc.ca
408 Bennett (n 310 above)229.

data privacy issues and proffering solutions on how they should be tackled.[409] It is therefore possible to conclude that in terms of intellectual debates on data privacy issues worldwide, the Privacy Commissioners have always contributed significantly. Perhaps, this is one of the reasons for the high level of awareness on data privacy issues in Canada.

4.5.1.5. The Privacy Commissioner as a policy adviser

Bennett points out that there is 'a fine line between the performance of wider educational and research roles, and the provision of advice on more specific projects and proposals'.[410] The Privacy Commissioner, in terms of both the Privacy Act[411] and PIPEDA,[412] is required to give advice or make a report to the government and organisations when formulating policies that impact on privacy.[413]

Recently, Daniel Therrien, the Privacy Commissioner, in a submission argued that a proposed Bill[414] 'is excessive and that it puts the personal information of Canadians at risk.'[415] He further contended that 'the bill could make available all federally held information about someone of interest to as many as 17 government departments and agencies with responsibilities for national security' without a limit on how such information is to be held.[416] Such is the policy advisory role of the Privacy Commissioner especially with respect to proposed legislation.

The role of policy adviser has an even more forceful effect in that it has, over time, been used to influence amendments of proposed legislation. For example, as a result of the 9/11 attacks in the US, the Canadian government (apparently persuaded by the US) introduced an Act to Amend the Aeronautics Act (Bill C-44) which will facilitate sharing of

---

409 Eg, see many of the works of David H Flaherty and Ann Cavokian who were both former provincial privacy commissioners.

410 Bennett (n 310 above) 229.

411 Privacy Act, sec 39(1).

412 Though not expressly contained in the PIPEDA, the Privacy Commissioner is required by sec 24 (d) to 'promote, by any means that the Commissioner considers appropriate, the purpose of [the law]'

413 See eg, Jennifer Stoddart's recommendations for reforms of the PIPEDA contained in a paper 'The Case for Reforming the Personal Information Protection and Electronic Documents' *Act* May 2013 https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp (accessed 1 November 2015).

414 Bill C-51, the Anti-Terrorism Act, 2015.

415 Office of the Privacy Commissioner of Canada 'Submission to the Standing Committee on Public Safety and National Security of the House of Commons' March 5, 2015. https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp (accessed 1 November 2015). See also 'C-51 anti-terrorism bill 'excessive,' Privacy Commissioner says' http://www.cbc.ca/news/politics/c-51-anti-terrorism-bill-excessive-privacy-commissioner-says-1.2984376 (accessed 1 November 2015).

416 Office of the Privacy Commissioner of Canada (n 415 above).

passengers' lists on flights entering or leaving Canada.[417] George Radwanski, a former Privacy Commissioner, expressed concerns over the proposed amendments and recommended 'an amendment that would restrict these agreement to share information collected for the purposes of protecting national security…'[418] His particular concerns were that the government of Canada will be a 'back-door beneficiary of this forced intrusion into the privacy rights of Canadians.'[419] The government in response initiated an amendment that will restrict the Canadian government from obtaining such information.[420]

4.5.1.6. The Privacy Commissioner as a quasi-judge

For the purpose of exercising the powers of a quasi-judge, it may be argued that Privacy Commissioner can try to resolve a complaint by any other alternative dispute resolution method outside litigation. In this case, various mechanisms are available such as negotiation, mediation and conciliation. A presentation by Foran, Rooke and Neary (all officials from the Privacy Commissioner's office) captures this role in an apt manner. The presenters observe that '[t]he federal Privacy Commissioner is an ombudsman - this role provides for reaching reasonable solutions by reasonable people…[which is] non-confrontational and non-adversarial...'[421] In fact, in exercising his/her duties as an Ombudsman, the Commissioner is, arguably, acting as a quasi-judge however without enforcement powers. Though without powers to make binding orders, the Commissioner can summon witnesses, administer oaths, compel production of evidence etc.[422]

4.5.1.7. The Privacy Commissioner as an Enforcer

Generally, as an ombudsman, the Commissioner has no enforcement powers to order an organisation to take a particular action.[423] He/she relies more on negotiation and persuasion.[424] Nevertheless, there are certain measures available to the Commissioner

---

417 Bennett & French (n 30 above) 8; in response to a law signed by George Bush which requires foreign airlines to supply passengers' personal information to US authorities. This is in disregard of sec 5 of the PIPEDA

418 Bennett & French (n 30 above) 8; this is contained in a letter written By George Radwanski to the Minister of transport. https://www.priv.gc.ca/media/nr-c/02_05_b_011130_e.asp (accessed 1 November 2015).

419 Bennett & French (n 30 above) 8.

420 Bennett & French (n 30 above) 8.

421 Office of the Privacy Commissioner (n 376 above).

422 Office of the Privacy Commissioner (n 376 above).

423 Office of the Privacy Commissioner (n 376 above).

424 Office of the Privacy Commissioner (n 376 above); see also Office of the Privacy Commissioner of Canada (n 415above).

which could be construed as an enforcement role. For example, if on investigation of a complaint, a *prima facie* case is established, the Commissioner shall provide the head of the institution with a report and, where appropriate 'request that ... notice be given … of any action taken or proposed to be taken to implement recommendations contained in the report'.[425] It is arguable, that the reaching of a decision contained in the report by the Commissioner is an act of enforcement of the law. Nonetheless, this request is at best subtle and persuasive in nature.

The forgoing analysis shows how important a DPA is in the enforcement and implementation of data privacy laws. Bygrave points out that having a DPA play a role in the enforcement of the law carries obvious advantages because they are 'appointed experts in the field.'[426] This is a reason why many data privacy laws put stringent qualification requirements on the office. Admittedly, data privacy law is not rocket science,[427] and as such any person with a legal background can hold the office, but Bennett observes:

> …gone are the days when the Privacy Commissioner can rely solely on legal expertise, applying the black letter of the law to each problem. Legal skills are, of course, a huge asset. But the modern Privacy Commissioner needs also to know about the range of other policy instruments that might be brought to bear on this increasingly challenging, complex and global problem, including public education, technological solutions, and management and accountability mechanisms.[428]

Part of the skill which the Privacy Commissioner must learn is the skill of persuasion since he/she does not have enforcement powers.[429] This therefore shows the critical role of the institution responsible for enforcement - the courts. It, however, by no means diminishes the relevance or importance of the DPA.

4.5.2. The role of the courts

Though decisions of DPAs are usually subject to judicial review, the role played by the courts varies from jurisdiction to jurisdiction. In many jurisdictions (typical EU archetypes), decisions of the DPA, insofar as they are legally binding, are subject to judicial review.[430] This is the limit of the role of the court in oversight and enforcement of

425 Privacy Act, sec 35(1).
426 Bygrave (n 38 above) 4.
427 Interview by Berzins with Flaherty. See Berzins (n 187 above).
428 Bennett (n 372 above).
429 Bennett (n 372 above). Unlike the provincial privacy commissioners who wield enforcement powers.
430 Bygrave (n 38 above) 169.

data privacy laws in these jurisdictions. In some other jurisdictions like Canada, however, courts play a more prominent role than as mere judicial reviewers, especially because the DPA do not exercise enforcement powers.

Under Canadian data privacy laws, the power of the court[431] is, arguably, activated on two conditions. Firstly, the power is triggered after the Commissioner has conducted an investigation and has arrived at a finding in a report (usually, the report contains the Commissioner's findings and recommendations). Secondly, if upon receipt of such a report, the organisation refuses to comply with the recommendation of the Privacy Commissioner, then court can Act. [432] Under the Privacy Act, there are various instances in which an individual can apply to the court for review.[433] In other circumstances, the Privacy Commissioner (with the consent of the individual) may apply or appear on behalf of the individual[434] or appear as a party.[435] The court can then make the necessary orders and award costs.[436]

Section 14 of the PIPEDA, however, provides for two (further) conditions to engage the jurisdiction of the court.[437] Firstly, the complainant must apply to the court for a hearing.[438] Secondly, the hearing must be in connection with any matter for which the complaint is made or that is referred to in the Commissioner's report.[439] A very important issue which borders on the overlapping role of the Privacy Commissioner and the court is whether a proceeding under section 14 of the PIPEDA is a review of the Privacy Commissioner's report (recommendations) or a *de novo* hearing by the court. In other words, is the court bound to give any weight to the report of the Privacy Commissioner when a complaint is before it? It seems that the court will take cognisence of the report of the Privacy Commissioner. In *Eastmond v Canadian Pacific Railway,*[440] however, it was held that proceedings under section 14 of PIPEDA is not a review of the Privacy Commissioner's

---

431 Privacy Act, sec 3 and PIPEDA, sec 2 says court means a Federal Court.

432 PIPEDA, sec 14 (or if the investigation has been discontinued by the Privacy Commissioner, sec 12.2(3)). See also Privacy Act, sec 41 & 42. The provision of the Privacy Act is limited as it is applicable only when access to documents in denied by the government department.

433 Privacy Act, sec 41 (when access is refused and time has lapsed), PIPEDA, sec 14.

434 Privacy Act, sec 42 (b) , PIPEDA, sec 15

435 Privacy Act, sec 42(c).

436 Privacy Act, sec 48 49 50, s 52 on cost; See PIPEDA, sec 16.

437 *Eastmond* (n 91 above) para 90.

438 *Eastmond* (n 91 above) para 90.

439 *Eastmond* (n 91 above) para 90, see also AZ Haque & MH Le 'Privacy year in review: Canada's Personal Information and Protection and Electronic Documents Act and Japan's Personal Information Act' (2004-2005) 1 *I/S: A Journal of Law and Policy for the information Society* 485.

440 (n 91 above), see generally Haque & Lee (n 439 above).

report (or recommendation), rather it is a fresh application which must be proved by the complainant.[441] The Federal Court further held that though the Privacy Commissioner's report was entitled to some deference for his specialised expertise, the hearing must be *de novo* in this case.[442] This decision shows that the court can exercise the full powers of the Privacy Commissioner especially where there is sufficient evidence before it.

In concluding this part, Bygrave's remarks on the importance of the court is apt. He points out that:

> [h]aving DPAs play the role carries obvious advantages - they are, after all, the appointed experts in the field. Yet there is also a risk that DPAs construe data privacy legislation in ways that further the cause of data privacy at the expense of other factors that require equal or greater weighting as a matter of *lex lata.* That risk is acute when promotion of data privacy is central to a DPA's formal remit. The judiciary, approaching the legislation with relatively fresh eyes and formally unencumbered by a pro-privacy mandate, will tend to be better able to resist such bias.[443]

4.5.3. A critique of the enforcement and oversight structure

The Canadian enforcement and oversight body has been very proactive in oversight and implementation of Canadian data privacy laws. In particular, the Office of the Privacy Commissioner is being very effective in its oversight function. This is borne out by two facts. Firstly, because of the high rating Canada has received in terms of data privacy protection in spite of the state of the Privacy Act.[444] Secondly, because of the enormous jurisprudence coming from the Office of the Privacy Commissioner on data privacy issues. The courts too have been very active in championing individuals' rights to data privacy as depicted by the number of cases they have decided on data privacy issues.

Nevertheless, the enforcement and oversight structure can be criticised for certain reasons. The lack of enforcement powers of the Privacy Commissioner has received the most criticism by commentators.[445] This has earned the Privacy Commissioner the status of a toothless and blind watchdog[446] and his recommendation - mere talks.[447] A recommendation, no matter how articulate, is ineffective without a corresponding power to

441 *Eastmond* (n 91 above) para 118.
442 *Eastmond* (n 91 above) para 123.
443 Bygrave (n 38 above) 4.
444 As discussed earlier in the introduction.
445 See Flaherty (n 93 above), Keith (n 219 above).
446 Berzin (n 187 above) 640
447 Keith (n 219 above).

enforce. Another weakness of the Privacy Commissioner's Office according to London is that, the office is not an independent agency.[448]

The court's role as an oversight and enforcement body has also been criticised.[449] Flaherty argues that the courts are inadequate as a vehicle for implementation of an important statute.[450] Another weakness is that, only the financially capable persons can bring an action before the court for a violation.[451] In addition, courts do not have the requisite technical and specialised knowledge to handle some of the data privacy issues brought before them.[452] But then, the court may arrive at a decision with guidance from the opinion of the Commissioner. The views of the Commissioner are, however, merely persuasive and the discretion of the judge is paramount.

A seldom considered weakness, is the multiple and complex nature of the structure. As seen in the provision of the laws (especially the Privacy Act), a lot of institutions have roles to play in data privacy issues.[453] This approach, though effective, could bring about confusion and duplication of roles. It could also lead to unnecessary bureaucracies. Thus, it may be difficult to implement this structure in developing countries that are still grappling with weak institutions, and as such does not provide a good example for developing countries like Nigeria.

4.6. Canada and international data privacy regimes: Extent of influences?

Canada is one of the non-European member countries of the Organisation for Economic Cooperation and Development (OECD). It is also a member economy of the Asia-Pacific Economic Cooperation (APEC).[454] Both international organisations have data privacy frameworks which, arguably, have some form of influence on the data privacy regimes of

448 London (n 60 above) 273. This is not surprising as both privacy laws have no provision requiring the Privacy Commissioner to be independent.

449 See Berzins (n 187 above) 636; Flaherty is one of the scholars who vehemently opposes the role of the courts.

450 Flaherty (n 355 above) 381.

451 Berzins (n 187 above) 637.

452 Berzins (n 187 above) 636; similarly, Bygrave contend that '…yet courts' frequent lack of familiarity with the legislation, combined with the time pressures of litigation, can result in their failing to appreciate the complexities of the legislation in ways that undermine the correctness of their judgments' Bygrave (n 38 above) 4.

453 As identified by Bennett above.

454 Both OECD and APEC and their data privacy framework have been considered in some detail in chapter 2 of this thesis.

member states. Likewise, Canada maintains an observer status in the parliamentary assembly of the Council of Europe.[455] It has, however, neither signed nor ratified the Council of Europe's Convention on Data Protection,[456] which makes it safe to submit that the Council's influence on data privacy protection in Canada is very limited.[457] But, the explanatory report to the Convention acknowledges Canada's participation in the preparatory works that brought about the Convention.[458]

With regard to the OECD, it is obvious that its Guidelines on data privacy have had a significant influence on data privacy legislation in Canada (and a lot of other data privacy legislation across the world).[459] The need for harmonisation of national data privacy legislation to enhance the free flow of personal data while upholding human rights, was the primary reason for developing the OECD Guidelines by member states.[460] Thus, the Guidelines represent 'a consensus on basic principles which can be built into existing national legislation.'[461] Consequently, most of the FIPs in Canadian data privacy legislation are similar to that of the OECD Guidelines.[462] Another salient influence the OECD Guidelines have on the Canadian data privacy framework, especially the PIPEDA, is in the approach of balancing commercial interest and the need for data privacy. In fact, one may argue that the PIPEDA primarily seeks to enhance consumer confidence in e-commerce so as to boost commercial activities. Such is in tandem with the overall

---

455 Canada was granted this status on 3 April 1996. See Resolution 96(9) on Observer Status for Canada with the Council of Europe. http://www.coe.int/t/der/docs/CMRes969Canada_en.pdf (accessed 1 November 2015). Observer status within the parliamentary assembly must be distinguished from an observer status *stricto sensu*. In the former, 'members of observer delegations may sit in the Assembly but without the right to vote. They have the right to speak with the authorization of the President of the Assembly.' See Council of Europe 'What is Observer status?' http://www.coe.int/en/web/portal/what-is-observer-status (accessed 1 November 2015).

456 http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG (accessed 1 November 2015).

457 For a list of conventions being ratified by Canada, see http://www.coe.int/en/web/portal/canada

458 COE 'The protection of individuals with regard to automatic processing of personal data in the context of profiling' 18 http://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf (accessed 1 November 2015).

459 T Banks '2013 OECD Privacy Guidelines- will Canada respond?' http://www.lexology.com/library/detail.aspx?g=c6df76c5-e982-4761-ba38-5cb49a08167e (accessed 1 November 2015).

460 Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 1 November 2015).

461 OECD (n 460 above).

462 See OECD 'Thirty years after the OECD Privacy Guidelines' (2011) http://www.oecd.org/sti/ieconomy/49710223.pdf (accessed 1 November 2015) 24; Quebec particularly adopted the FIPs of the OECD Guidelines. Holmes (n 96 above) 2.

objectives of the OECD Guidelines.[463] The OECD generally encourages international cooperation between member countries for the purposes of facilitating transborder data flows. In so doing, member states are encouraged to refrain from restricting transborder data flows.[464] This is wholly consistent with Canada's approach of placing little or no restriction on transborder data flows. Finally, the OECD Guidelines do not refer to sensitive data or automated processing. There are, however, various sections suggesting 'different protective measures' are applicable based on the sensitivity of personal information.[465] This is also found in the major data privacy laws in Canada.

The OECD Guidelines have not only influenced national data privacy frameworks, but also other international data privacy frameworks. This is more noticeable with the APEC Privacy Framework, which has been described by Greenleaf as 'OECD lite'.[466] The APEC Privacy Framework came into force in 2004 making its influence on substantive contents of the Canadian data privacy laws minimal as influences, in this regard, cannot be in retrospect.[467] There are, however, some APEC initiatives which seek to enhance data privacy protection in member economies.[468] Recently, APEC initiated a Cross-border Privacy Enforcement Arrangement (CPEA) which 'creates a framework for regional cooperation in the enforcement of Privacy Laws.'[469] The aim of the CPEA is 'to contribute to consumer confidence in electronic commerce involving cross-border data flows by establishing a framework for regional cooperation in enforcement of privacy laws.'[470] Participation of Canada in the APEC's CPEA system has numerous advantages as identified by Heyder.[471] Part of the benefits include: facilitating legal compliance,

---

463 See generally part III of the Guidelines which focuses on encouraging free flow of personal data.

464 See eg, part IV secs 17 & 18 of the revised Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013). OECD (n 460 above).

465 OECD (n 462 above) 20.

466 See G Greenleaf 'APEC's privacy framework sets a new low standard for Asia-Pacific' in AT Kenyon & M Richardson (eds) *New dimensions in privacy Law: International and comparative perspectives* (2006) 96. Also 7 of the 21 APEC economies are also members of OECD.

467 The latest of Canadian data privacy law, the PIPEDA was enacted in 2001.

468 Usually, state parties of APEC are called member economies.

469 APEC Cross-border Privacy Enforcement Arrangement (CPEA). http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx (accessed 1 November 2015). It was endorsed by APEC Ministers in November 2009 and commenced in July 2010.

470 CPEA (n 469 above).

471 M Heyder 'The APEC Cross-Border Privacy Rules – Now that we've built it, will they come? *Privacy Perspectives* September 4, 2014 https://privacyassociation.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come/ (accessed 1 November 2015); Canada's application for participating in the CBPR was favourably considered by The Joint Oversight Panel (the JOP) on 1st April 2015. Canada is the 4th country to join this scheme after US, Mexico and Japan. It was stated that Canada's joining will 'strengthen the system.' 'Asia-Pacific: Canada's joining of APEC CBPRs will

transborder data transfers, creating consumer trust, aiding investigations and enforcement.[472] The system promises to be viable for transborder data transfers in the APEC region.

Without doubt, interaction between Canada and international data privacy frameworks has further enriched the regime in one way or the other. Nevertheless, the forgoing international instruments are not the only ones that have had an influence on the Canadian data privacy regime. The EU Directive, arguably, has also been influential in the data privacy regime of Canada. This will now be considered.

4.7. The European Union Commission's 'adequacy' finding on data (privacy) protection in Canada

Obviously, one of the primary reasons for enacting data privacy laws in many countries is because of the influence of the EU Directive which has been a global pacesetter in the field. Article 25 of the Directive specifies that personal data can be transferred from any European country to a third country only if the third country has an adequate data privacy regime.[473] Article 25(6) empowers the commission to make such decisions. Some exceptions are provided for where personal data can be transferred to a country without an 'adequate', regime, but this is a more cumbersome process.[474] Because of the force of the adequacy requirement and the 'might' of the EU in terms of trade, many countries strive to attain a positive finding from the EU. In fact, the provision has been the primary reason for some countries enacting data privacy legislation.

The same may also be said of the Canadian regime, especially the PIPEDA. Arguably, one of the main reasons for the enactment of the law was so as to obtain an adequacy finding from the EU and thereby boost commerce.[475] In 2004, the Canadian data privacy framework (PIPEDA) was assessed by the European Commission (assisted by a non-

'strengthen the system'http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3615 (accessed 1 November 2015).

472 Hyder (n 471 above).

473 EU Directive, art 25 (1).

474 EU Directive, art 26.

475 B Schwartz 'Canada's new privacy law: Strategies for compliance' (2002) 2 *Asper Review of International Business and Trade Law* 125.

binding opinion of the Article 29 Working Party) and found to be adequate.[476] It was the view of the commission that:

> The Canadian Act covers all the basic principles necessary for an adequate level of protection for natural persons, even if exceptions and limitations are also provided for in order to safeguard important public interests and to recognise certain information which exists in the public domain. The application of these standards is guaranteed by judicial remedy and by independent supervision carried out by the authorities, such as the Federal Privacy Commissioner invested with powers of investigation and intervention. Furthermore, the provisions of Canadian law regarding civil liability apply in the event of unlawful processing which is prejudicial to the persons concerned.[477]

Two important observations are discernible from the opinion of the EU Commission above which may serve as a basis for lesson-drawing. Firstly, the FIPs in a law are very crucial in determining the strength and quality of a data privacy regime. Secondly, the quality of implementation and enforcement of these principles also goes to establishing an adequate regime. Thus, it is not enough for the data privacy instrument to provide for the best of standards in terms of the principle without supporting it with effective implementation mechanisms.

Article 4 of the opinion states that '[t]he Commission shall evaluate the functioning of this Decision on the basis of available information, three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of the Directive…'[478]. Based on this provision, a subsequent assessment was carried out by the European Commission, and it was found that 'the Canadian Personal Information and Electronic Documentation Act continues to provide an adequate level of protection of personal data within the meaning of Article 25 of the Directive.'[479]

---

476 European Commission (EC) 'Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act' http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0002&from=EN (accessed 1 November 2015).

477 EC(n 476 above).

478 EC(n 476 above).

479 Council of the European Union 'The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act' 22 November 2006 http://ec.europa.eu/justice/policies/privacy/docs/adequacy/canada_st15644_06_en.pdf (accessed 1 November 2015).

The adequacy finding of the Canadian regime is strictly on the PIPEDA. Hence, it does not cover the Privacy Act and other provincial legislation. Nevertheless, with respect to provincial legislation, the European Commission is of the view that 'it is foreseen that when the Canadian Government recognises a provincial law as being substantially similar to (PIPEDA), the Commission's decision will be adapted to reflect this.'[480]

The adequacy finding by the EU obviously makes Canada a reference point in the North American region in particular, and the world in general, on data privacy issues. Despite its complex approach to data privacy protection, it has still earned the approval of the rigorous regime of the EU. That notwithstanding, the Canadian regime is not perfect and that is why it needs to undergo certain reforms in the future.

4.8. Proposals for legislative reforms of data privacy laws in Canada

Legal developments in the area of data privacy law are in a constant state of flux worldwide.[481] Constant technological developments always challenge the extant rules and make the laws on data privacy obsolete. Policymakers must, accordingly, acknowledge this fact and put in place machineries to update their legal regimes so that the laws can keep pace with rapid advances in technology. Thus, while there is much to learn from the existing framework on data privacy in Canada, there is equally much more insight to gain from proposed legal reforms on data privacy in Canada. This part briefly highlights some of the proposals for legal reforms and the particular issues in the Canadian data privacy regime they focus on.

With Regard to the PIPEDA, there are three recent attempts at reforms stemming from the 2006 PIPEDA review.[482] In September 2011, the Canadian government introduced the Safeguarding Canadians' Personal Information Act (Bill C-12)[483] which is still pending before Parliament. Some of the reforms proposed by the Bill include: exclusion, in certain

---

480 European Commission 'Frequently asked questions on the Commission's adequacy finding on the Canadian Personal Information Protection and Electronic Documents Act' http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq_en.htm (accessed 1 November 2015); see also McWilliam (n 40 above) 1993.

481 Siegel (n 225 above) 307, Bennett (n 310 above) 230.

482 Sec 29 of the PIPEDA provides that Part 1 of the PIPEDA is to be reviewed after every 5 years. See Lithwick (n 194 above) 2.

483 Bill C-12 An Act to Amend the Personal Information Protection and Electronic Documents Act http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5144601 (accessed 1 November 2015); This Bill came before parliament first as Bill C-29 (An Act to amend the Personal Information Protection and Electronic Documents Act.

circumstance, of business contact information;[484] clarifying elements of a valid consent for processing of personal information;[485] and permitting the disclosure of personal data without knowledge and consent of the individual for certain purposes.[486] The most important proposal for amendment is the requirement of data breach notification.[487] The second proposal for reforms came in 2013 with Bill C-475[488] which essentially seeks to, among others, give the Privacy Commissioner order-making powers and enhance the power of the courts to impose fines in cases of non-compliance.[489] The Digital Privacy Act (Bill S-4)[490] is the latest attempt to update Canada's private sector law.[491] Lithwick highlights some of the proposed amendments introduced by the Bill.[492] These include permitting disclosure of individuals' personal data without knowledge and consent in certain circumstances; requiring organisations to take some steps in cases of data security breaches and creating offences for failure to comply with obligations on data security breaches.[493]

The bulk of the arguments for legal reforms is centred on the antiquated Privacy Act.[494] Flaherty observes that '[t]he Privacy Act is a twenty-five year old house that had little maintenance and refurbishment. It is now ripe for a major rehab job. Fiddling with the paint, or redecorating one room, will not do the job.'[495] According to Holmes, calls for

---

484 (n 483 above), sec 4; this is necessary as the PIPEDA has been earlier criticised on the grounds that there are no rules on the sale of business. See Keith (n 219 above).

485 (n 483 above), sec 5.

486 Eg, for the purposes identifying an injured, ill or deceased individual' performing policing services, preventing, detecting fraud or protecting victims of financial abuse. See generally Bill C-12 (Historical) Safeguarding Canadians' Personal Information Act https://openparliament.ca/bills/41-1/C-12/ (accessed 1 November 2015).

487 A compulsory obligation on organisations to inform data subjects or Privacy Commissioner of a breach of security of personal data immediately it occurs. Sec 10.1

488 Bill C-475 An Act to Amend the Personal Information Protection and Electronic Documents Act (Order-Making power) http://www.parl.gc.ca/legisinfo/BillDetails.aspx?Language=E&Mode=1&billId=5996156 (accessed 1 November 2015).

489 (n 488 above)

490 Introduced in the Senate in 2014 Available at http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6524312&File=27#1 (accessed 1 November 2015).

491 M Geist 'Why the Digital Privacy Act undermines our privacy: Bill s-4 risks widespread warrantless disclosure' April 10 2014 http://www.michaelgeist.ca/2014/04/s-4-post/ (accessed 1 November 2015).

492 Lithwick (n 194 above).

493 Lithwick (n 194 above) 1, for more insightful analysis of the draft bill, see Lithwick (n 194 above).

494 Though I will not want to re-emphasise the issues as areas of flaws have been identified when carrying out an analysis of the Act in parts 4.4.2 of this chapter.

495 A similar observation was made by Stoddart. See Office of the Privacy Commissioner of Canada 'The necessary rebirth of the Privacy Act' 29 November 2013 https://www.priv.gc.ca/media/sp-d/2013/sp-d_20131129_02_e.asp (accessed 1 November 2015). She stated that 'time has come to stop trying to patch up this first generation privacy legislation. It needs to be reborn'.

reforms of the Privacy Act dates as far back as 1987 with a report titled *Open and shut: enhancing the right to know and the right to privacy*.[496] A similar effort was made in 1997 with a report titled *Privacy: where do we draw the line?*[497] Jennifer Stoddart, in 2006, made a comprehensive proposal for reforms of the Act.[498] Particular areas of reforms identified in the report include broad conceptual changes to the Act;[499] extending its scope; [500]and strengthening the Act.[501] The proposal was further substantiated with an addendum in 2008.[502] While awaiting a 'comprehensive modernization' of the Privacy Act, the Office of the Privacy Commissioner (based on the 2006 proposal), proposed '10 quick fix changes for the Act'.[503] In 2009, the House of Commons Standing Committee on Access to Information, Privacy and Ethics issued its report suggesting partly that some of the issues raised should be considered at a later date.[504] Unlike the PIPEDA, there are no draft bills proposing reforms of the Privacy Act.[505]

4.9. Chapter conclusion: The art of lesson-drawing from Canada?

This chapter investigated the insights that can be gained from the Canadian experience on data privacy protection. In doing this, the researcher focused on the data privacy legislation at the federal level. The analysis was carried out based on the adequacy assessment criteria of the EU Commission (via Article 29 WP) which focuses on the contents of the law

496 Holmes (n 96 above) 10.
497 Holmes (n 96 above) 10.
498 This was contained in a report titled 'Government Accountability for Personal Information: Reforming the Privacy Act' June 2006 https://www.priv.gc.ca/information/pub/pa_reform_060605_e.asp (accessed 1 November 2015). This was in a presentation to the House of Commons Standing Committee on Access to Information, Privacy and Ethics.
499 This comprises of reconsidering the Ombudsman model and research and public education functions.
500 This comprises of expanding the jurisdiction of the Act, protecting unrecorded information, strengthening court review, extending Access rights etc.
501 This largely includes reconsideration or strengthening of the FIPs.
502 Privacy Commissioner of Canada 'Addendum to government accountability for personal information: reforming the Privacy Act' April 2008 https://www.priv.gc.ca/information/pub/pa_ref_add_080417_e.pdf (accessed 1 November 2015).
503 They quick fix changes are: to create a legislative 'necessity test' which would compel government departments to show the purpose of collecting personal information; expanding the grounds for application for court review; establishing privacy impact assessment; providing the Commissioner with explicit educational and awareness mandate and bestowing him/her with more powers to report publicly on privacy management practices of government institution; providing more discretion for the Commissioner to refuse and/or discontinue complaints; amending the Privacy Act to align with the PIPEDA by eliminating restriction to only recorded information; strengthening annual report requirement; introducing requirement on five years compulsory review and tightening the provisions governing disclosure of personal information to foreign states. See Office of the Privacy Commissioner of Canada 'Privacy Act reforms' https://www.priv.gc.ca/parl/2008/parl_080429_02_e.asp (accessed 1 November 2015).
504 Office of the Privacy Commissioner (n 492 above).
505 Office of the Privacy Commissioner (n 492 above).

(especially the strengths of the FIPs) and the enforcement (oversight) mechanism. The analysis was carried out with a view to identifying the salient and significant features of the Canadian legal regime on data privacy and to establish what lessons can be drawn by Nigeria in developing a framework on data privacy. As a prelude to this discussion, the chapter analysed the nature of data privacy issues in Canada and tried to establish a link to what obtains in Nigeria so as to justify the choice of Canada for this study. The main issues identified which threaten the right to data privacy in Canada were similar in some ways to that of Nigeria. They include processing of personal information for commercial purposes in the private sector and law enforcement purposes in the public sector. The response of the Canadian government to national security issues and the pressures from the US further heightens threats to data privacy in Canada. Nigeria, like Canada, is also facing a lot of security challenges which have made individuals' right to data privacy to be increasingly under threat.

Another important issue considered in this chapter is the conceptual basis and approach to data privacy in Canada. Discussion of this issue also, tried to justify the choice of Canada for this research. In this regard, it was argued that Canada adopts a 'middle ground' between the EU and the US approaches. The regime falls between the EU over-protectionist and the US *laissez-faire* approaches. This middle ground approach is influenced by the conceptual basis of data privacy in Canada. Unlike the US that protects data privacy for liberty and EU for dignity, Canada protects data privacy for autonomy and control. This is, indeed, relevant for data privacy protection in Nigeria.

The analysis of the legal framework for data privacy in Canada started with the constitutional provision. It was noted that unlike Nigeria, the courts are ready to extend the constitutional provision on privacy to protecting personal information even though the right to privacy is not expressly contained in the Canadian Constitution. To further enhance data privacy protection in Canada, the Supreme Court of Canada stated that the issues of data privacy have a quasi-constitutional status. This is a very vital insight for Nigeria. With respect to statutory protection of data privacy, the laws on the private and public sectors were analysed. Special consideration was also given to the health sector because of the myriad of issues that personal health information provokes. A combination of historical, analytical and comparative methodologies was adopted in this regard so as to expound useful lessons for Nigeria. Issues considered in both laws include their historical

basis, scope, the FIPs, rights and duties, exemptions and transborder data flow regime. Based on a critical examination of these laws, it was concluded that although the PIPEDA has a commercial agenda, the Privacy Commissioner and the courts have been proactive to ensure that consumers' adequately protected from threats resulting from their data processing. While the PIPEDA tries to achieve a high standard of privacy protection, the same cannot be said of the Privacy Act. It was argued, however, that lesson can still be drawn from its regime. Particular weaknesses of the Act were identified which are largely as a result of its lack of review. The Privacy Act therefore depicts the necessity for regular review of a data privacy policy and legal framework.

Based on the requirement of the EU Commission's adequacy requirement, the chapter also critically examined the oversight and enforcement structure of data privacy law in Canada. It was submitted that the unique structure of this mechanism presents vital insights for any jurisdiction. The Privacy Commissioner plays a crucial role and has a wide range of policy instruments to ensure compliance with the law. He/she does not, however, have an enforcement power which is a major weakness. The courts enforce data privacy law but may give deference to the opinion of the Privacy Commissioner contained in his/her report, especially because of the Commissioner's expertise in the field.

The interaction between Canada and international data privacy frameworks has, in one way or the other, enriched its legal regime and this is a useful lesson. The OECD Guidelines, particularly, have been influential in data privacy law in Canada. Similarly, the APEC has measures in place to ensure a high level of compliance with its standards by member economies. Canada belongs to both organisations and has therefore been influenced by their frameworks. The EU Directive has also been influential in the private sector, even though Canada is not a member state of the EU. The EU Commission's adequacy decision in regard to data privacy in Canada's private sector was analysed briefly. Based on the decision, this researcher observes that a great deal of consideration is given to the strengths of the FIPs in the law and the level of enforcement and oversight of the law.

While admitting that no data privacy regime is perfect, some efforts at legislative reforms of data privacy laws in Canada were identified. In this regard, the chapter notes that that for a data privacy law to be effective in responding to contemporary challenges, it must be periodically reviewed. The Privacy Commissioner's role in this respect is noteworthy. This

is another vital insight to be derived from Canada's experience on data privacy protection. On the whole, the Canadian regime on data privacy presents a number of useful lessons for Nigeria. Another country's regime that appears promising in terms of data privacy protection is South Africa. The next chapter, therefore, scrutinises the South African experience on data privacy protection.

Chapter five

An analysis of the legal framework for the protection of data privacy in South Africa: Lessons for Nigeria

5.1. Introduction

> *…it must again be emphasised that since the activities of the data industry create a huge threat or potential threat to personality interests, the traditional common law principles of protecting privacy and identity (which are still in their infancy) are unable to deal effectively with the problems in this field, and many countries may require adequate data protection in South Africa for the continuous free cross-border flow of personal information from them to our land, the adoption of legislation is necessary.*[1]

The previous chapter analysed the legal regime for the protection of data privacy in Canada where it was observed that, in line with international practice, the trend is protecting data privacy using the constitution and statutory instruments.[2] South Africa, too, has recently designed its data privacy framework following this trend with the enacting of the Protection of Personal Information Act ('POPIA' or 'the Act')[3] which is anchored in

1 J Neethling *et al Neethling's law of personality* (2005) 281.

2 Eg, in the previous chapter, it was shown that the Canadian legal framework for data privacy protection is both the Canadian Charter and the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). Though the European Union (EU) is not a sovereign independent entity, its framework also shows a similar approach. The Charter of the Fundamental Rights of the European Union 2000/C 364/01 ('EU Charter') and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ('EU Directive') (soon to be replaced with the 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 (draft EU Regulation)) are the main instruments on data privacy.

3 Act 4 of 2013. Also available at http://www.justice.gov.za/legislation/acts/2013-004.pdf (accessed 1 November 2015).

the South African Constitution.[4] This may partly be as a result of the weaknesses of the previous approach of protecting data privacy using traditional common law principles as acknowledged by the scholars in the quotation above.[5] Another possible explanation for the increasing trend of jettisoning the common law/civil law in protecting data privacy in many jurisdictions, including South Africa, may be the increasing realisation of the differences between 'private information' and 'personal information'.[6] Common law principles may be suitable for protecting the former, but not the latter.[7]

This chapter, therefore, adopts the approach of the previous chapter in carrying out an analysis of the extant legal framework for protecting data privacy in South Africa with a view to obtaining useful insights for Nigeria. The chapter focuses largely on the constitutional and statutory protection of data privacy.[8] The analysis in this chapter will begin in part 5.2 with a brief overview of the nature and challenges of data processing in South Africa. This discussion is carried out with a view to showing that similar data processing activities, with related risks, obtain in both South Africa and Nigeria. The chapter then proceeds in part 5.3 to investigate the conceptual basis and approach to data privacy protection in South Africa. An analysis of the conceptual basis of data privacy

---

4 See POPIA, the preamble & sec 2(a).

5 Neethling (n 1 above) 281. See also AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law and Security Report* 79 where he observes that 'common law of Africa has not been and still does not constitute sound [data] privacy protection.'

6 Eg, Black explains the power of personal data in contemporary time. He states that '[i]n the last forty years, the power of information has increased exponentially. Previously, information only wielded power if sufficiently intimate or personal [confidential]. Eg, in the 1960s, the average person with a [sic] only a phone number could use that information for any purpose other than to call the individual to whom the number belonged. Now, the same person with only a phone number could retrieve a name and address with minimal effort over the internet. With the name, address, and phone number, the person holds sufficient information to retrieve further data from government agencies, such as public records and criminal history. Therefore, with each piece of information provided to the government or private firms, the individual yields significant power to that entity.' RB Black 'Legislating US data privacy in the context of National Identification Numbers: Models from South Africa and the United Kingdom' (2001) 34 *Cornell International Law Journal* 437. More on the differences between private information and personal information has been discussed in chapter one of this thesis. However, preliminary analysis of the differences, see R Wacks *Personal information privacy and the law* (1989) 21-25.

7 These arguments on the weaknesses of the common law in protecting personal data *stricto sensu* have been made in chapter 3 above. See particularly secs 3.4.3 & 3.4.4. More will be discussed in this chapter.

8 The works of legal scholars such as Professors Johann Neethling and Anneliese Roos have largely focused on protection of personal data under the law of delict, thus the discussions will not be repeated in this chapter. See Neethling (n 1 above), A Roos 'The law of data (privacy) protection: A comparative and theoretical study' unpublished LLD thesis, University of South Africa, 2003 543-651. Also see other more specific works that discuss elements of data privacy protection under the common law such as DJ McQuoid-Mason 'Consumer protection and the right to privacy' (1982) 15(2) *The Comparative and International Law Journal of Southern Africa* 135-157.
This chapter will also not discuss much on other laws that have provisions on data privacy protection. The laws have been elaborately considered in Roos (n 8 above) 653-717.

protection in the country will be carried out for two reasons. Firstly, understanding the conceptual basis exposes the underlying reasons for the approach. Secondly, the discussions on the conceptual basis will justify the choice of South Africa for the purpose of this study.

Based on the foundation laid above, an analysis will be carried out in part 5.4 of the legal regime of data privacy in South Africa. Similarly, part 5.5 considers the (proposed) oversight and enforcement mechanism of data privacy law in the country. In part 5.6, selected topic areas that are currently generating global debate, and their provision in the POPIA, will be analysed to show how the Act seeks to adapt to contemporary data processing challenges. Furthermore, a general critique will be carried out of the (proposed) regime of the POPIA in part 5.7. The critique is for the purpose of predicting the prospects and challenges of the Act in realising adequate data privacy protection in South Africa. In concluding this chapter in part 5.8, the extent of the influence of international (and regional) data privacy regimes on South Africa (if any) will be examined.

A limitation of the chapter, particularly in discussing the POPIA, is that the legislation is relatively new which means that there is no case law and not so much scholarly literature on it. Nevertheless, this does not constitute a challenge as such for the purpose of lesson-drawing for Nigeria for two reasons. Firstly, the POPIA (as will be seen shortly) has been substantially influenced by other existing and longstanding international data privacy frameworks.[9] Secondly, many insights can be obtained from the contents of the law itself, particularly the fair information principles (FIPs).[10]

5.2. The nature and challenge of data processing in South Africa: Any similarity with Nigeria?

Neethling identified a number of data processing activities in South Africa which constitute threats to data privacy right. He, however, noted that 'the list must not be

---

9 Such as the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 1 November 2015); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) http://conventions.coe.int/treaty/en/Treaties/Html/108.htm (accessed 1 November 2015) and the EU Directive.

10 Moreover, quite a number of Roos's works discussed the Protection of Personal Information Bill which subsequently became the Act with very little modifications. See eg, A Roos 'Data protection' in D Van der Merwe *et al Information and communications technology law* (2008) 367-389.

regarded as exhaustive, as other controllers also exist or may be created.'[11] Based on Neethling's exposition, certain data privacy activities in the private and public sectors threaten the right to data privacy.[12] The state, with its numerous departments and agencies, is the data privacy user in the public sector, and personal information is required for several purposes which include law enforcement, taxation and population census.[13] The likelihood of personal information being used for other purposes outside that for which it was collected is the major data privacy challenge in the public sector. This becomes increasingly so with greater information sharing between the public and private sectors.

With respect to private entities [14] in South Africa, '[t]he most important private data users are credit bureaux, transport companies, the health and medical profession, banks and financial institutions, the insurance industry, and the retail and direct marketing industry.'[15] Credit bureaus[16] seem to present the greatest challenges to data privacy in this category. They obtain personal information from various sources, some of which may be inadequate and can affect the accuracy of information collected.[17] Some authors have also identified other challenges of data processing in various activates and/or sectors. In the health sector, for example, Ferraud-Ciandet, in a comparative study of South Africa and France, has shown how health data of patients are circulated via web applications, telephone and videoconferences.[18] The concerns that arise with the application of health care systems which are based on personal information were identified by the author. Black

11 Neethling (n 1 above) 268.
12 Neethling (n 1 above) 268.
13 See generally Neethling (n 1 above) 269-270.
14 Neethling used the term 'private data controllers'.
15 See South African Law Reform Commission (SALRC) 'Privacy and data protection report' (2009) para.1.2.9 available at www.justice.gov.za/salrc/dpapers/dp109.pdf (accessed 1 November 2015).
16 As of 2009, there are 11 known credit bureaus in South Africa. See SALRC (n 15 above) para 5.3.9 'South African credit bureaus have records on 19.5 million credit-active consumers. The number of consumers with impaired records increased to 46 percent – or a staggering nine million consumers – in the first quarter of 2012. Breaking down the 46 percent, almost 20 percent of consumers are three months or more in arrears; 12 percent have an adverse listing at a credit bureau; and 14 percent of consumers have judgments or administration orders against them.' See A Arde 'Find out what creditors say about you' http://www.iol.co.za/business/personal-finance/financial-planning/financial/find-out-what-creditors-say-about-you-1.1341085#.VW6zlc-qqko (accessed 1 November 2015). Perhaps that is a reason why a dedicated legislation contains elaborate provisions on the protection of personal information in the hands of Credit Bureau. See the National Credit Act, Act 34 of 2005. For discussions on the Act, see Roos (n 10 above) 364-367.
17 Eg, relying on information collected about an individual from newspapers or old records.
18 N Ferraud-Ciandet 'Privacy and data protection in eHealth: A comparative approach between South African and French legal systems' (2010) IST-Africa 2010 conference proceeding P Cunningham & M Cunningham (eds) *International Information Management Corporation* 2010. Also available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=5753017 (accessed 1 November 2015)

considered the challenges of national identification numbers on data privacy.[19] He observes that 'the prevalent use of national identification numbers triggers an imminent privacy crisis regarding control of information.'[20] Millard discussed the impact of unsolicited communications in the form of cold-calling on individuals' data privacy rights.[21] Several other works have identified data privacy challenges in a wide range of sectors, such as the credit industry,[22] insolvency situations,[23] banking[24] and broadcasting.[25]

The surge in the use of the internet in South Africa also presents specific challenges to data privacy as in Nigeria. Ncube posits that South Africa is the most internet connected country in Africa[26], and, as such, it faces similar (data) privacy challenges with other

19 Black (n 6 above).

20 Black (n 6 above)398.

21 D Millard 'Hello, POPI? On cold calling, financial intermediaries and advisors and the Protection of Personal Information Bill' (2013) 76 *Tydskrif vir hedendaagse Romeins-Hollandse Reg (THRHR)* 604-622. The author was of the view that '[u]nsolicited communications from services providers probably qualify as the single biggest irritation known to those who use telephones and email.' 605. His analysis in the article was based on practice of cold calling in the case of *The Registrar of Financial Services Providers v Catsicadellis and Botha* Enforcement Committee Case No 6 of 6 November 2012.

22 McQuoid-Mason contends that '[i]n many cases an action for invasion of privacy is sufficient to protect an individual against intrusions and publicity. With the development of computer and the increasing use of databanks, however, the efficacy of the action may be threatened. This is particularly true in respect of consumers who enter into credit dealings with private sector or make use of certain state facilities. McQuoid-Mason (n 8 above) 136.

23 Smith discusses the challenge of data privacy in cases of insolvency. He particularly focuses on the implication of personal information of customers in a customer list which the debtor must have accumulated over a long period of time 'by promising each customer that his or her information would not be disclosed to other persons without his/her consent.' Data privacy challenge, therefore, arises if the liquidator wishes to sell such valuable list. See A Smith 'Privacy and the sale of customer lists in South African insolvency law. Some issues reconnoitred' (2004) 16 *South African Mercantile Law Journal* 598-621.

24 See NT Masete 'The challenges in safeguarding financial privacy in South Africa' (2012)7(3) *Journal of International Commercial Law and Technology* 248-259. She contends that '[s]ome financial institutions would abuse their customers' information by providing third parties with it without their customers' consent.' 253. See also FS Cronje 'A synopsis of proposed data protection legislation in SA' (2007) 4(4) *Journal of Digital Forensics, Security and Law* 43-50.

25 The tension between freedom of expression and the right to privacy also constitutes a challenge to data privacy in South Africa as is typified by a number of cases like *Tshabalala-Msimang v Makhanya 2008* (6) SA 102 (W). Pressmen unlawfully accumulate and disclose individual's personal and private information and courts hold that such act does not constitute a violation of the right to data privacy because it will amount to unjustifiable censorship. Thus, it has been argued that the POPIA will restrict a broadcaster's right to freedom of expression. Visser, therefore, expresses the view that '[a]n approach that balances media freedom and privacy is essential for the development of a legal framework that can appropriately curtail the possible chilling effect created the Bill [POPIA]' C Visser 'The protection of personal information in broadcasting: The effect of the Protection of Personal Information Bill on freedom of expression' (2011) 27 *South African Journal of Human Rights* 343.

26 CB Ncube 'Watching the watcher: Recent developments in privacy regulation and cyber-surveillance in South Africa' (2006) 3(4) *SCRIPT-ed* 345. See also RW London 'Comparative data protection and security law: A critical evaluation of legal standards' unpublished LLD thesis, University of South Africa, 2013 367.

advanced countries.[27] For example, recent reports in South Africa showed that a large number of websites collect personal data.[28] Another prominent effect of the proliferation of the internet in South Africa (like Nigeria) is the spread in the use of Social Networking Services (SNSs). Roos analysed the impact of Facebook[29] on data privacy rights and observed that Facebook may not be as private as people think despite their numerous privacy policies.[30] It is submitted that most of the challenges to data privacy stated above also obtain in Nigeria with varying impact.[31]

5.3. The conceptual basis and approach to data privacy protection in South Africa

Quite a number of reasons influenced the choice of South Africa for the purpose of this study. Besides the fact that South Africa is a developing country experiencing similar threats to data privacy as Nigeria, the conceptual basis for data privacy in the country will present useful insights for Nigeria. Like Nigeria, South Africa is a multicultural country with a federal system of government hence, its approach to data privacy will be a useful case study. In addition, South Africa has a more developed privacy culture when compared to other African countries.[32] This is more so for data privacy which has developed over time and has a rich source of jurisprudence in the law of delict.[33] The level of awareness of the value of controlling the processing of one's personal data seems to be higher in South Africa[34] than in other Sub-Saharan countries as depicted by available case law.[35] This

---

27 Ncube (n 26 above) 345. Her discussion is, however, centered on the challenge of reconciling online privacy with freedom of expression with the need to fight cyber-crime and terrorism. In fact, a recent survey shows that across 13 different countries shows that a strong majority of the population view internet access as a fundamental right in developing countries like South Africa and India. See S Dutta *et al* 'The new internet world, a global perspective on freedom of expression, privacy, trust and security online' in the Global Information Technology Report 2010-2011 9. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1916005 (accessed 1 November 2015).

28 London (n 26 above) 368.

29 Facebook is said to be 'South Africa's most popular social network'. It has been ranked as 'the number one social platform in South Africa with 11.8 million users.' Other SNSs like YouTube, Twitter, Mxit, LinkedIn and Instagram have a total number of 7.2, 6.6, 4.9, 3.8 and 1.1 million respectively. See 'Facebook South Africa user numbers' http://businesstech.co.za/news/internet/72266/facebook-south-africa-user-numbers/ (accessed 1 November 2015).

30 A Roos 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *The South African Law Journal* 375-402.

31 This has been discussed in detail in chapter 3 of this thesis.

32 AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) *International Data Privacy Law* 175.

33 See note fn 95 below.

34 According to London, '[r]esearch on public concerns regarding data protection and security concerns in SA has occurred over time. A survey conducted in SA [South Africa] revealed that seventy three percent of those sampled reported concerns about the loss of control over their personal information.' London (n 26 above) 368; See also Roos (n 8 above) 659.

value 'is particularly significant because in the absence of the value that supports the existence of privacy laws, efforts to enact such laws are likely to remain of little or no significance.'[36]

South Africa has adopted the 'EU model' of data privacy protection with a comprehensive law (the POPIA) that regulates the public and private sector data processing activities. [37] In South Africa, however, no watertight distinction is made between the rights to privacy and data (privacy) protection unlike in the EU.[38] Data privacy is an integral part of the right to privacy referred to as *information privacy*.[39] As noted in chapter two,[40] in Europe, there is currently a growing body of jurisprudence and scholarship that seeks to remove data privacy totally from the realms of privacy.[41] Nevertheless, it is submitted that South Africa's approach is, at least, in line with the plain wording of the EU Directive where the right to privacy is reasonably tied to data protection.[42] The draft EU Regulation, however, adopts a different approach, in that privacy and data protection are totally separated.[43]

Because of the substantial influence the EU data privacy regime has on South Africa, it may be argued that the conceptual basis for data privacy is the same in both jurisdictions. As we have stated in the previous chapter, data privacy in the EU is for the purpose of

---

35 Makulilo (n 5 above) 80.

36 AB Makulilo *Privacy and data protection in Africa* (2014) back cover page.

37 See SALRC (n 15 above) viii. See also K Allan & I Currie 'Enforcing access to information and privacy rights: evaluating proposals for an Information Protection Regulator for South Africa' (2007) 23 *South African Journal of Human Rights* 563-564. Adoption of this model is not surprising as the EU is South Africa's largest trading partner. See MJ Calaguas 'South African Parliament enacts comprehensive data protection law: An overview of the Protection of Personal Information Bill' (2013) 3 *Africa Law Today* 5.

38 See O Lynskey 'Deconstructing data protection: the 'Added-value' of a right to data protection in the EU Legal order' (2014) *International and Comparative Law Quarterly* 569-597. See also M Tzanou 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right' (2013) 3(2) *International Data Privacy Law* 88-99. LA Abdulrauf 'Do we need to bother about protecting our personal data? Reflections on neglecting data protection in Nigeria' (2014) 5(2) *Yonsei Law Journal* 78-81.

39 More on data privacy as an integral part of privacy will be discussed in sec 5.4.1 of this chapter. Suffice it to mention at this point that this understanding (of data privacy as a sub-category of privacy) has its merits. There are, however, some clear challenges in this approach. This is because making data privacy a sub-category of privacy may restrict its scope of protection to private or confidential information only which we have argued is more restricted than personal information.

40 See chapter 2, 2.7.

41 One of the strongest voices on the issue of distinguishing privacy from data protection in the EU is that of De Hert and Gutwirth. See P De Hert & S Gutwirth 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action' in S Gutwirth et al (eds) *Reinventing Data Protection*? (2009) 8-10. More elaborate discussions on this issue were carried out in chapter 2 of this thesis.

42 See EU Directive, art 1.

43 See draft EU Regulation, art 1(2). Compare with n 42 above.

protecting the dignity of Europeans.[44] Similarly, human dignity is a core value in the South African Constitution[45] and has substantially influenced every right in the Bill of Rights.[46] Thus, data privacy as an integral part of privacy is also for the purpose of promoting dignity.[47] Nevertheless, South Africans, like Canadians, also worry about the processing of their personal data by both public and private entities. It seems, however, that South Africans, like Europeans, worry more about the processing of their personal data by private entities.[48]

One issue which is seldom considered by African data privacy scholars (on the conceptual basis of data privacy in South Africa) is the influence of African culture[49] on its (data) privacy regime. It may be argued that data privacy is 'human rights' and 'technology-centred' and, as a consequence, outside the realms of culture.[50] Olinger *et al* investigate the extent of the influence of the western notion of privacy and *Ubuntu*[51] on the South African

---

44 A Levin & M J Nicholson 'Privacy law in the United States, the EU and Canada: Allure of the middle ground' (2005) 2 *University of Ottawa Law & Technology Journal* 391

45 It is usually referred to as *Ubuntu*. See sec 1 of the South African Constitution which listed human dignity as one of the core values upon which the Republic of South Africa is founded. Dignity is also given a central place in the preamble of the Constitution. See LM du Plessis 'The evolution of constitutionalism and the emergence of a constitutional jurisprudence in South Africa: An evaluation of the South African Constitutional Court's approach to constitutional interpretation' (1999) 62 *Saskatchewan Law Review* 315.

46 Sec 7(1) of the South African Constitution provides that '[t]his Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom.'

47 In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) also available at http://www.saflii.org/za/cases/ZACC/2000/12.pdf ; Langa DP was of the view 'that privacy is a right which becomes more intense the closer it moves to the intimate personal sphere of the life of human beings, and less intense as it moves away from that core. This understanding of the right flows…from the value placed on human dignity by the Constitution.' Para 18. Based on this reasoning, Currie and de Waal concluded that perhaps the principal value served by privacy is human dignity. I Currie & J de Waal *The Bill of Rights handbook* (2005) 320. See also A Hughes *Human dignity and fundamental rights in South Africa and Ireland* (2014) 264.

48 This is justified by the discussions preparatory to the Act as shown in the SALRC discussion paper (n 15 above). See also Levin and Nicholson (n 44 above) 391.

49 It may be argued that there is nothing like a universal African culture. Africa is a multicultural society with multiple cultures and traditions. For the purpose of discussion in this part, African culture is used to refer to the collective native laws and customs in Africa as against the western culture, especially, of the colonialists.

50 Another argument is that issues of privacy are foreign to African culture and tradition which is collective in nature. Issues of data privacy and culture were discussed in chapter 3 above. See also Hughes (n 47 above) 72.

51 In *S v Makwanyane* 1995 6 BCLR 665 (CC) para 224. Also available at http://www.saflii.org/za/cases/ZACC/1995/3.pdf. Langa J explained the concept of *Ubuntu* in very apt words. He contended that 'It [*Ubuntu*] is a culture which places some emphasis on communality and on the interdependence of the members of a community. It recognises a person's status as a human being, entitled to unconditional respect, dignity, value and acceptance from the members of the community such person happens to be part of. It also entails the converse, however. The person has a corresponding duty to give the same respect, dignity, value and acceptance to each member of that community. More

Protection of Personal Information Bill (now Act).[52] With regard to the influence of the western notion of privacy on the POPIA, there is no controversy. After all, privacy laws are all about promoting individuality through the control of the use and disclosure of one's personal information. The controversial aspect is the influence of *Ubuntu* on the POPIA which may *prima facie* seem contradictory as African culture is less individualistic than western culture and directed more towards ensuring the benefits of the common good.[53] In this regard, Hughes contends that, '*Ubuntu* recognises the dignity of individuals in the context of the common good'.[54] Privacy 'might [thus] be regarded as not being beneficial for the good of the community.'[55] Olinger *et al*, therefore, admitted that *Ubuntu* may not have a direct influence on the POPIA.[56] Nevertheless *Ubuntu* is similar to the EU culture of privacy which is one of protection of human dignity[57] and the EU culture of privacy has, in turn, substantially influenced the POPIA. On that basis, the scholars (Olinger *et al*) concluded that '[w]e are of [the] opinion that *Ubuntu* will find its place and influence in the Bill, and eventually the Act in an indirect manner via the concept of human dignity.'[58]

The next part of the chapter will consider the practical application of *Ubuntu* in promoting human dignity within the constitutional provision on privacy and POPIA. It must be stated that, since South Africa has a similar conceptual basis and approach to data privacy protection as the EU, numerous references will be made to the EU instruments (both the Directive and draft Regulation) in explaining data privacy principles.

---

importantly, it regulates the exercise of rights by the emphasis it lays on sharing and co-responsibility and the mutual enjoyment of rights by all.'

52 HN Olinger *et al* 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 *The International Information & Library Review* 31-43.

53 Olinger (n 52 above) 34. See also Hughes (n 47 above) 72.

54 Hughes (n 47 above) 72.

55 Olinger (n 46 above) 35.

56 Olinger (n 46 above) 40 for discussions on the reasons.

57 Olinger (n 46 above) 40.

58 Olinger (n 46 above) 42.

5.4. The legal framework for the protection of data privacy in South Africa

5.4.1. Protection of data privacy under the South African Constitution

Two provisions in the Bill of Rights of the South African Constitution could be linked to the *sui generis* right to data privacy. They are sections 14 and 32.[59] The analysis in this part will focus on the former as it forms the normative basis of the right to data privacy in South Africa.[60] Section 14 provides that '[e]veryone has the right to privacy, which shall include the right not to have (a) their person or home searched; (b) their property searched; (c) their possession seized; or (d) the privacy of their communications infringed.[61] The South African Constitutional Court points out that '[t]hese rights flow from the value placed on human dignity.'[62] Currie and De Waal, in analysing section 14, posit that it has two parts.[63] The first part, which is contained in the opening phrases, guarantees a general right to privacy.[64] 'The second [part] protects against specific enumerated infringements of privacy, namely searches and seizures of someone's person, property or possessions and infringements of the privacy of communication.'[65] Analysing section 14 in this way may be overly simplistic and it makes the guarantee and protection of data privacy (as narrowly construed) doubtful under the South African Constitution.

In another vein, Roos,[66] relying on McQuoid-Mason,[67] opines that the constitutional right to privacy can be divided into 'substantive privacy rights'[68] and 'informational privacy

---

59 This is without prejudice to the general role of human dignity as a core value of the South African Constitution and the Bill of Rights as discussed in 5.3 above. Sec 32 provides for the right of access to information. It provides that '[e]veryone has the right of access to (a) any information held by the state; and (b) any information that is held by another person and that is required for the exercise or protection of any rights'. For more on the importance of sec 32 to the right to data privacy protection, see J Burchell 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13(1) *Electronic Journal of Comparative law* 14; see also Roos (n 8 above) 658-659.

60 This does not, however, undermine the provisions of sec 32 above. See POPIA, sec 2(a).More discussions on this will be carried out shortly.

61 See *The Teddy Bear Clinic for Abused Children & Anor v Minister of Justice and Constitutional Development & Ors* (2013) ZACC 35. Also available at http://www.saflii.org/za/cases/ZACC/2013/35.pdf. *Thint (Pty) Ltd v National Director of Public Prosecutions & Ors: Jacob Gedleyihlekisa Zuma, Hully v National Director of Public Prosecutions & Ors (2008)* ZACC 13 Case CCT 89/07 http://www.saflii.org/za/cases/ZACC/2008/13.pdf on the importance of search warrants See also *Hyundai* (n 47 above).

62 See *Thint (Pty)* (n 61 above) Langa CJ in para76. See also *Bernstein and Others v Bester and Others NNO* 1996 (2) SA 751 (CC).

63 Currie & de Waal *The Bill of Rights Handbook* (2013) 302-303.

64 Currie & de Waal (n 63 above) 302-303, South African Constitution, sec 14.

65 Currie & de Waal (n 63 above) 302-303.

66 Roos (n 30 above) 395.

rights'.[69] With regard to 'informational privacy rights' (which is the focus of this discussion), Neethling's definition is apt as it has been adopted by the South African Constitutional Court.[70] He opines that:

> Privacy is an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those *personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private*.[71] [Emphasis added].

This definition upholds the right to data privacy (informational privacy) as an integral part of the right to privacy.[72] Currie and de Waal, relying on the decision of the South African Constitutional Court in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit,*[73] contend that '[t]he right to privacy should be interpreted as protecting an individual's interest in what has been called 'informational self-determination'.[74] Informational self-determination, according to them, is 'an interest in restricting the collection, use of and disclosure of personal information.'[75] Based on this interpretation, it is submitted that

---

67 DJ McQuoid-Mason 'Invasion of privacy: common law v constitutional delict—does it make a difference?' (2000) 227 *Acta Juridica* 248

68 According to McQuoid-Mason, substantive privacy rights, which he refers to as 'personal autonomy privacy case', 'enables individuals to make personal decisions about such interests as their family relationships, home life and sexual orientation, eg possession of pornography and the practice of sodomy' (n 67 above) 248.

69 See also M Gondwe 'The protection of privacy in the workplace: a comparative study' unpublished PhD thesis, University of Stellenbosch, 2011 61. She opines that sec 14 of the Constitution has 'has created new classes of privacy rights. The new classes of rights created by the constitutional are substantive and informational privacy rights. Substantive privacy rights protect "personal autonomy" whereas informational privacy rights "prevent [disclosure] and access to information".' She relied on A Devenish *Commentary on the South African Bill of Rights* (1999) 147. In the SALRC report three broad groups of privacy were identified. They are protecting privacy against intrusion into private life; disclosure of private facts and infringement of autonomy. (n 15 above) 29.

70 *Bernstein AO v Bester NO AO & NM AO v Smith AO* 2007(7) BCLR 751 (CC) at para [34] Currie prefers to call this conception of privacy 'the Neethling's common-law conception' which is also 'informational self-determination'. See I Currie 'The concept of privacy in the South African Constitution: Reprise' (2008) 3 *TSAR* 549.

71 The definition was first proposed in Prof Neethling's thesis. See Neethling J '*Die Reg op Privaatheid*' Unpublished LLD thesis University of South Africa 1976 though in Afrikaans. For the English version of his views, see Neethling (n 1 above) 270. There are, however, many disputes among South African jurists about the proper conceptualisation of the constitutional right to privacy. For a more in-depth analysis and a cross section of the views of the major scholars, see Currie (n 70 above) 549-557.

72 See CM van der Bank 'The right to privacy - South African and comparative perspectives' (2012) 1(6) *European Journal of Business and Social Sciences* 78; SALRC (n 15 above) 2.

73 No 2001(1) SA 545 (CC); Ncube also relying on this case opines that '[e]ven though not explicitly mentioned within the language of the section these protections extend to the breach of informational privacy'. See C Ncube 'A comparative analysis of Zimbabwean and South African data protection systems' (2004) 2 *The Journal of Information, Law and Technology.*

74 Currie & de Waal (n 63 above) 302-303. See also Hughes (n 47 above) 265.

75 Currie & de Waal (n 63 above) 302-303.

section 14 provides for the right to data privacy.[76] In this regard, the influence of the EU is seen in the concept of informational self-determination which has a European origin.[77]

De Waal and Currie point out the need for this category of privacy (information privacy) in the contemporary digital society. They are of the opinion that 'the importance of legal protection for this aspect of privacy has increased as technological advances … have facilitated the collection, dissemination and interception of personal information in electronic form.'[78]

The views above have demonstrated the willingness of the Constitutional Court of South Africa[79] and jurists to expand and enrich the jurisprudence on human rights in the country. Despite their inherent conservatism, the courts have been able to stretch the constitutional provision so as to accommodate contemporary challenges brought about by advances in technology. This is indeed an extremely useful lesson for a country like Nigeria.

The Bill of Rights in the South African Constitution operates both vertically and horizontally.[80] An individual can enforce his right to data (information) privacy against other individuals and the state.[81] In addition, the South African constitutional provision is very insightful as the use of the term 'everyone' means even non-South Africans can

---

76 This is further justified by the decision of the Constitutional Court in the Case of *Mistry v Interim National and Dental Council of South Africa (*1998) (4) SA 1127 (CC) [51]. Also available at http://www.saflii.org/za/cases/ZACC/1998/10.pdf. The case was based on sec 13 of the Interim Constitution which has similar provisions with sec 14 of the current Constitution. Sachs J in the case refrained from making a full analysis of the dimension of the right to information privacy. He also observed that the terrain (of information privacy) is complex and controversial. See para 47 of the judgment page 49-50. The SALRC states that '[s]ection 14 will, however, not only have an impact on the development of the common law action for invasion of privacy. It may also create a new constitutional right to privacy.' (n 15 above) 29

77 Informational self-determination originated for the German population census decision. Informational self-determination, even though not contained in the EU Charter, is said to be the basis for the right to data privacy protection in the EU. Lynskey (n 38 above) 591. On the *German Census case* see G Hornung & C Schnabel 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25(1) *Computer Law & Security Review* 84.

78 Currie & de Waal (n 63 above)303.

79 For more on the creative use of the judicial authority of the Constitutional Court to advance substantial justice as a feature of transformative constitutionalism, see E Christiansen 'Transformative Constitutionalism in South Africa: Creative uses of Constitutional Court authority to advance substantive justice' (2010) 13 *The Journal of Gender, Race & Justice* 575-614.

80 South African Constitution, sec 8. Based on secs 8(2) & (3), the Bill of Rights applies to both natural and juristic persons. See McQuoid-Mason (n 67 above) 228. See also Van der Bank (n 72 above) 79; Burnchell (n 59 above) 4.

81 Hughes, however, notes that different obligations may be imposed on an individual and the state especially where financial expenditure is involved. See Hughes (n 47 above) 130.

benefit from the constitutional protection of data privacy.[82] Nevertheless, the Constitution only lays down the framework or basis for balancing competing interests like the interest of an individual to have control over the processing of his/her personal information and other people's (business entities) interest in such information.[83] There was, therefore, the need for an explicit legislation to balance both interests (that of the individual and the data processors) while ensuring that the human rights of individuals prevail.[84] In another vein, Neethling argues that 'the entrenchment of the right to privacy in section 14 of the Constitution places an obligation on the legislature to initiate [further] steps in this regard.'[85] This is because the South African Constitution provides that 'the state must respect, protect, *promote and fulfil* the rights in the Bills of Rights' (emphasis added).[86] The South African legislature has taken steps in that regard by enacting a law. Obviously, Nigeria can draw some lessons from the South African experience in this respect. Hence, the next part of the chapter will focus on the legislation.

5.4.2. Statutory protection of data privacy: The Protection of Personal Information Act (POPIA) 2013

Recently, the South African legislature enacted the POPIA.[87] Before the passing of the Act, however, certain principles in the common law of delict on personality protection were applicable for the protection of (data) privacy in South Africa.[88] For liability under the law of delict to arise, the infringement of (data) privacy must be wrongful and unreasonable.[89] Liability, under the law of delict, also arises only in cases of a wrongful act which is intentional.[90] Mere negligence cannot make a defendant liable under the law of delict.[91] The requirement restricts the individual's right as liability under the data privacy law, *stricto sensu*, is strict, that is it can arise without negligence or fault.[92] In this

---

82 See AB Makulilo 'Protection of personal data in sub-Saharan Africa' published Dr. Jur. thesis, University of Bremen, 2012 396.
83 See SALRC (n 15 above) vi, 4.
84 SALRC (n 15 above) 5.
85 Neethling (n 1 above) 271. Roos (n 10 above) 354.
86 See South African Constitution, sec 7(2) See also Neethling (n 1 above) 272.
87 No 4 of 2013.
88 Neethling (n 1 above) 272.
89 The so-called *contra bonos mores*. Neethling (n 1 above) 273; Hughes (n 47 above) 261; see also SALRC (n 15 above) para 2.3.11.
90 Neethling (n 1 above) 273.
91 *NM v Smith* (n 89 above) para 55.
92 See Milliard (n 21 above) 618. See also J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of delict' (2012) 75 *Tydskrif vir hedendaagse Romeins-Hollandse Reg* (*THRHR)* 247. The Court of Justice of the European Union (CJEU) also reached a similar conclusion in the *Google Spain case.* In the case, the court was of the view that an entity which processes personal

regard, Neethling observes that the processing of personal data poses a serious threat to a person's personality in 'that it is probably fair and justifiable to hold a data institution liable even where intention or negligence is not present.'[93] Moreover, liability for the invasion of privacy covers only the violation of information which a person considers to be private, secret or confidential and not necessarily 'personal information' as applicable under data privacy law.[94] In a nutshell, the traditional principles of the law of delict are largely limited as they do not grant an individual *active control* over his/her personal information, which means he/she has less control over the processing of his/her personal data.[95] Controlling the processing of one's personal data, as we have argued earlier, is the crux of the *sui generis* right to data privacy.[96] After evaluating the law of delict on protection of data privacy, therefore, Roos concluded that, though South Africa has a well-developed level of protection for privacy and identity in the law of delict,[97] it does not provide sound data (privacy) protection.[98]

The law of delict was not the only legal structure for the protection of data privacy in the pre-POPIA era. Several other laws, mostly sectoral, also applied with various overt

---

information is a 'data controller' with the context of the EU Directive irrespective of 'knowledge' and 'intention'. See Case 131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos and Mario Costeja González* (2014) ECR I-000 (nyr).34. (Google Spain case). See also commentaries on the case in O Lynskey 'Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78(5) *The Modern Law Review* 524.

93 Neethling (n 1 above) 278.

94 See O'Regan's view in *NM v. Smith* (n 89 above) para 142-143 where she opined that '…it should be emphasised that a court should not lightly conclude that what is a private fact has been rendered a public fact simply because a small number of people may have come to know of it. The question will be one of fact, in particular, whether the fact has been disclosed to such an extent that, viewed objectively, it can no longer genuinely be considered to be private.'

95 Neethling (n 1 above) 273.

96 See chapters 1 & 2.

97 A Roos 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 11 *Potchefstroom Electronic Law Journal* 92. Roos's view on the level of development of the delictual principles on privacy seems to be in contrast with that of Neethling who believes delictual principles are still in their infancy. Neethling (n 1 above) 272. See also opening quotation to this chapter. (n 1 above).

98 And she, therefore, called for the enactment of a legislation to grant individuals enhanced control over the processing of their personal information. See Roos (n 95 above) 92; Roos (n 10 above) 358. See also Makulilo (n 5 above) 79. The inadequacy of the common law principles of delict to adequately provide remedy for data privacy violations is so in spite of the provisions of sec 173 of the South African Constitution which requires the court to develop the common law taking into account the interest of justice. Perhaps the provision of sec 173 of the Constitution is a reason why Van der Merwe opposes the idea of a legislation on data privacy. See Neethling (n 1 above) 273 fn 65. In the case of *H v W* 2013 (2) SA 530 (GSJ) also available at www.saflii.org/za/cases/ZAGPJHC/2013/1.pdf, Willis J pointed out lapses of the common law on privacy especially with regard social networking. He contended that '[i]t is in respect of the remedy where infringements of privacy take place in the social media that the common law needs to develop' Page 21. See also SALRC (n 15 above) para 2.4.3.

weaknesses.[99] These laws are the Promotion of Access to Information Act (PAIA),[100] the Electronic Communications and Transactions Act (ECTA),[101] and the National Credit Act.[102] The laws were basically not able to meet up with the challenges of the present day personal information problem. This presented a platform for the emergence of the POPIA.[103]

5.4.2.1. The POPIA in historical perspective: Lessons from the law-making process

Enacting a law is a quite a rigorous process. A law on data privacy is even more difficult because of the complexities involved.[104] This is reflected in the process leading up to the POPIA. Stein aptly states that

> [t]he Protection of Personal Information Bill (POPI)… has been one of the longest serving bills before the parliament. The lengthy and detailed deliberations on the Bill have, however, allowed the drafters to draw on the experience of many years of data protection regulation in the European Union,

---

99 For more elaborate discussions of this law and criticism thereof, see A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* 400.

100 The Promotion of Access to Information Act 2 of 2000. In the first place, the PAIA is a freedom of information and not a data privacy law. Although, PAIA promotes some of the objectives of data privacy, it is inherently limited in adequately providing for the right to data privacy. See generally Roos (n 10 above) 368-360. For more on the right to access to information in South Africa, See I Currie 'Scrutiny: South Africa's Promotion of Access to Information Act' (2003) 9(1) *European Public Law* 59–72.

101 Act 25 2002. A limitation of the Act, in terms of sec 50 (1), is that it is applicable only to personal information obtained in the course of electronic transactions. See Ncube (n 26 above) 345. According to Roos, perhaps the 'major deficiency of the ECT Act is the fact that it does not impose legally binding obligations on data controllers. Subscription to the principles enumerated in sec 51 is voluntary. Should the controller decide to subscribe to the principles, a breach of them will only amount to breach of contract with the data subject.' Similarly '[t]here is no external supervisory body or criminal sanctions to enforce the principles.' Roos (n 10 above) 364.

102 Act 34 of 2005. This Act has a strict sectoral application. It applies only to personal information in the credit industry though it has been stated that 'the National Credit Act is probably the most successful in its attempt to introduce data-protection provisions.' See Roos (n 10 above) 367.

103 Obviously, the weaknesses of the common law in adequately protecting data privacy in the era of big data and increasing computerisation made Professor J. Neethling call for a legislation on data protection in his PhD thesis as far back as 1976.

104 Kuner opines that '[d]ata protection law is a mixture of various legal areas, such as human rights law, public law, private law, and others' C Kuner 'An international legal framework for data protection: Issues and prospects' (2009) 25(4) *Computer Law & Security Review* 315. Bygrave also opines that data privacy law straddles the boundaries between public and private law, criminal and civil law. See LA Bygrave 'Determining applicable law pursuant to European data protection legislation' (2000) 16 *Computer Law & Security Report* 252–257; P De Hert & V Papakonstantinou 'The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 also briefly discusses the difficulties of data privacy legislating with regard to the EU Directive and draft EU Regulation. So much policy, cultural and conceptual considerations are also involved in data privacy legislating.

> including the comprehensive review of EU data protection law that is currently underway by the European Commission.[105]

Based on Stein's contention above, quite a number of useful insights can be obtained with respect to the law-making process of the POPIA.[106] The first lesson is the long-time taken in discussion and deliberations on the draft law.[107] The process, which started as far back as 2000, culminated only towards the end of 2013.[108] What does this timespan say? The length of time taken is indicative of the rigorous process involved in terms of research, discussions, meetings and presentations. The task of formulating the law was bestowed on the South African Law Reforms Commission (SALRC or the Commission) which is the body 'to do research with reference to all branches of the law of the Republic and to study and investigate all such branches in order to make recommendations for the development, improvement, modernisation or reform thereof.'[109] The committee had broad terms of reference to investigate all aspects of the right to data privacy and recommend any legislative or other step to be taken.[110] The published discussion paper,[111] which led to a report (Project 124 *Privacy and data protection)* of 860 pages, shows the nature of the research that was carried out. Considerable literature was consulted with sufficient debate on the proposed provisions of the Bill by relevant stakeholders.[112] This is not surprising as the project committee comprised of erudite scholars in the field of privacy and information law, like Professors Johann Neethling and Iain Currie.[113] The discussion paper was widely

---

105 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). Although there is no mention of the proposed review in the SALRC report.

106 For the purpose of obtaining insights, only key issues which ought to be considered will be highlighted and contextualised. This part will not go into details on the law making process of the POPIA. For elaborate analysis on this, see SALRC (n 15 above) 1.

107 This is reflected in the numerous discussion papers on the topic.

108 On 17 November 2000 the SALRC considered and approved investigations into privacy as part of its programme. SALRC (n 15 above) 1. In fact, till today, the law in full is yet to come into force.

109 South African Law Reforms Commission Act, 19 of 1973, sec 4. See also SALRC 'About' http://www.justice.gov.za/salrc/about.html (accessed 1 November 2015).

110 SALRC (n 15 above) 13.

111 SALRC (n 15 above) 13.

112 Calaguas (n 37 above).

113 The Members of the committee are Prof Iain Currie, Ms Caroline da Silva, Ms Christiane Duval, Prof Brenda Grant, Ms Adri Grobler, Mr Mark Heyink, Ms Saras Jagwanth and Ms Allison Tilley. Professor Neethling was the leader of the project. See SALRC (n 15 above) 2. Ms Ananda Louw carried out most of the research work for the committee.

published (at every stage)[114] and serves as useful research material for policymakers and legal scholars.[115]

The research process in designing the POPIA also shows that a conscious effort was made to draw from the experiences of other jurisdictions that have longstanding data privacy regimes.[116] The final report of the research group revealed a very careful assessment and evaluation of provisions in data privacy laws across the world. The EU was a particular point of reference in this regard. The drafting process not only took note of the existing EU framework but also of the future data privacy instrument which is still being debated by the EU Commission.[117] Milo and Palmer posit that, '[t]he delay in its [POPIA] enactment can be attributed in part to the publication of the draft EU General Data Protection Regulation as the POPIA drafting Committee paused to consider some of the proposed innovations in that Regulation.'[118] This shows the importance of comparative studies and lesson-drawing in formulating data privacy laws.[119]

Another important lesson from the law making process is the wide consultation that was undertaken by the project committee.[120] Even the SALRC admitted that, '[t]he recommendations and draft legislation are the result of a very thorough consultation process'.[121] This is because the task of balancing opposing interests is a delicate one which requires thorough consultation.[122]

---

114 The first was published in September 2003 and is available on the SALRC website. South African Law Reform Commission Privacy and Data Protection Project 124 Issue Paper 24 September 2003 available at http://www.doj.gov.za/salrc/index.htm; subsequently in 2005; another discussion paper with a draft of the legislation was published for general information and comments. See South African Law Reform Commission 'Privacy and data protection' Project 124 Discussion Paper 109 October 2005 available at http://www.justice.gov.za/salrc/dpapers/dp109.pdf . The Final report was presented to the SALRC in 2009. See SALRC (n 15 above).

115 SALRC (n 15 above) para 1.4.1 &1.4.2.

116 Especially from European, North American and certain Asian countries like the Netherlands, Germany, USA, Canada, and Australia.

117 Stein (n 105 above).

118 D Milo & G Palmer 'South Africa- New comprehensive data privacy law passed' *Linklaters* 31 January 2014 available at http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-News-31-January-2014/Pages/SouthAfrica-New-comprehensive-data-privacy-law-passed.aspx (accessed 1 November 2015).

119 SALRC (n 15 above) para 9.1.1.

120 See SALRC (n 15 above) 651-654 for list of persons and entities consulted.

121 SALRC (n 15 above) ix

122 SALRC (n 15 above) para 1.2.29 & 1.2.30.

Be that as it may, deliberations on the POPI Bill were concluded, and it was passed into law in November 2013 following the President's signature.[123] The Act is to commence on a date to be determined by the President by proclamation in the government Gazette.[124] Certain provisions of the Act, however, came into force on proclamation by the President in April 2014.[125] The rest of the chapter will focus on particular provisions of the Act.

5.4.2.2. Purpose/objectives of the POPIA

The objective of the POPIA has been succinctly captured in section 2. The Act is first to 'give effect to the constitutional right to privacy' of a data subject[126] by protecting personal information being processed by a responsible party.[127] This objective is, however, not absolute as the Act immediately recognises the need for 'justifiable limitations' in exercising the right to privacy. These limitations include the need to balance the privacy right against other rights, particularly the right to freedom of information and the necessity to safeguard the interest of the free flow of information within and outside South Africa.[128] This provision (section 2) upholds the normative basis of the right to data privacy which is found in the constitutional right to privacy, and it has unequivocally shown that the POPIA is an instrument that seeks to balance the various interests of individuals. These interests include promoting accountability in government by not unduly restricting access to information and freedom of expression. It also includes the interest in processing of personal information of other entities (private and public).[129]

---

123 On the 26 November 2013. See *Data protection laws of the world: South Africa* available at http://dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=ZA (accessed 1 November 2015).

124 See POPIA, sec 115

125 The provisions which came into effect include the definition section and the provisions on the establishment of the office of the Regulator. See Data protection laws of the world (n 123 above) 1.

126 Sec 1 of the POPIA defines a data subject as 'the person to whom information relates'. This definition is similar to what obtains in the EU Directive (art 2). The draft EU Regulation, however, gave an elaborate definition of data subject which recognises the contemporary challenges of the online environment art 4 EU Regulation. See also De Hert & Papakonstantinou (n 104 above) 133. It is the researcher's view that the EU Regulation's approach is preferable to the POPIA which merely gives a very simple and brief definition of data subject. This is because of the need for contemporary data privacy regulation to focus more on the individual rather that the personal data.

127 POPIA, sec 2.

128 POPIA, sec 2. See also R Luck 'POPI- Is South Africa keeping up with international trends' (May 2014) 541 *De Rebus* 45 also available at http://reference.sabinet.co.za/webx/access/electronic_journals/derebus/derebus_n541_a26.pdf (accessed 1 November 2015).

129 The terms 'processing' and 'personal data' will be explained in the next part of the chapter. Suffice it to mention at this point that they are both technical terms with very specific application under the POPIA. Unlike some other data privacy interests, this objective which Bygrave categorises as a 'less formal

Other objectives of the POPIA include: to regulate, in harmony with international standards, the processing of personal information; [130] to provide individuals with rights and remedies for unreasonable processing of their personal data;[131] and to establish measures to promote, fulfil and realise the right to data privacy which includes the establishment of an Information Regulator.[132]

According to the SALRC, the purpose clause is crucial to the POPIA for two reasons.[133] Firstly, it outlines the general philosophy of the Act which means that, in their interpretation of any provision in the Act, the courts should be guided by the purpose clause.[134] Secondly, the purpose clause is important in a principle-based piece of legislation because of the need for constant interpretation and application of principles in the legislation to particular contexts.[135] Be that as it may, section 2 is not the only reference point in determining the philosophy of the Act. The courts may also be guided by the title of the POPIA, especially because of its very elaborate provision.[136] It is, however, submitted that the title of the POPIA is too detailed compared with other contemporary data privacy legislation.[137] Most of the contents of the title are already provided for in the purpose clause, and it appears to be repetitive.[138]

---

aim' of data protection law is prominent in the object clause of the POPIA. LA Bygrave *Data privacy law: An international perspective* (2014) 121.

130 POPIA, sec 2(b).

131 POPIA, sec 2(c).

132 POPIA, sec 2(d).

133 SALRC (n 15 above) para 3.2.1.

134 SALRC (n 15 above) para 3.2.1. See also POPIA, sec 3(3)(a).

135 SALRC (n 15 above) para 3.2.2.

136 POPIA, title. The long title is 'Act to promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Assess to information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across borders of the Republic; and to provide for matters connected therewith.'

137 Eg, the long title of the Data Protection Act of Ghana 2012 is simple 'An Act to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters.'

138 Even the EU privacy instruments (EU Directive and Regulation) do not have a title as long as this very long title of the POPIA. It may be argued that the EU Directive is merely a directive, and it is left for member states to provide for the principles of data protection in their laws. Nevertheless, the EU Regulation is meant to be directly applicable to member states.

5.4.2.3. Jurisdiction and application of the POPIA

The existence of personal information generally triggers the application of a data privacy regulatory regime.[139] With respect to the POPIA, the existence of personal information, together with the presence of certain conditions, activates its jurisdiction. In terms of section 3(1), the POPIA applies to the *processing* of *personal information* 'entered into a record[140] by or for a responsible party[141] by making use of automated or non-automated means'.[142] Where, however, the recorded personal information is processed by automated means, the POPIA applies only 'if it forms part of a filing system[143] or is intended to form part thereof'.[144] With regard to the territorial scope of the POPIA, it goes without saying that the POPIA applies only where the data processing is carried out in South Africa. This means the responsible party must be domiciled in South Africa.[145] There is no evidence suggesting that the Act applies extraterritorially. From the provisions of the POPIA, it is also clear that it protects the personal information of South African citizens and non-citizens in so far as the responsible party carries out the processing in South Africa. The view justified by the fact that there is nothing in the definition of either a 'data subject' or

---

139 PM Schwartz & DJ Solove 'Reconciling personal information in the United States and European Union' (2014) 102 *California Law Review* 879 wherein the opinion was expressed that personal data 'is foundational to any privacy regulatory regime because it serves as a jurisdictional trigger: if there is PII [personally identifiable information], the laws apply. If absent, the [data] privacy regulation does not apply.' See also PM Schwartz & DJ Solove 'The PII problem: Privacy and a new concept of personally identifiable information' (2011) 86 *New York University Law Review* 1814. See also Bygrave, (n 129 above) 129 where he contends that '[d]ata privacy law generally applies to 'personal data' or information.'

140 A record is defined by the POPIA as 'any recorded information regardless of the form or medium'. It includes writing on any material, information produced recorded or stored by means of various electronic devices including the computer; book, map drawing, etc.

141 A responsible party in terms of the sec 1 of POPIA is 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.' By this definition, the POPIA has avoided the confusing distinction between a 'controller', 'processor' and 'third party' that the EU Directive and draft EU Regulation maintains. (See art 2 of EU Directive and art 4 of the draft EU Regulation). Thus, liability for every data processing is carried by the responsible party alone. Sec 20 of the POPIA, however, talks about an operator. Nevertheless, the responsible party is generally responsible for data processing of the operator. Moreover, the line of divide between the responsible party and the operator may 'increasingly become blurred in an interconnected world of ubiquitous computing' See De Hert & Papakonstantinou (n 104 above) 135. See also European Commission Communication from the commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions 'A comprehensive approach on personal data protection in the European Union'. Available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (accessed 1 November 2015) para 2.2.4.

142 POPIA, sec 3(1).

143 A filing system 'means any structured set of personal information, whether centralised, decentralised or dispersed on functional or geographical basis, which is accessible according to specific criteria'. See POPIA, sec 1.

144 POPIA, sec 3(a).

145 POPIA, sec 3(b)(i).

'personal information' which suggests that only South Africans should be protected. Moreover, the right to privacy under the South African Constitution, which is the basis of the POPIA, applies to both citizens and non-citizens.[146] The POPIA, however, also applies where the responsible party is not domiciled in South Africa but makes use of automated or non-automated means in South Africa.[147] Such automated or non-automated means used in the country must not, however, be for the purpose of forwarding personal information through South Africa.[148] Thus, if South Africa is not the final destination but merely a transit region of the personal information, the POPIA is inapplicable.

Section 3(1) of the POPIA has adopted some key terms which must be present for the law to be applicable. These terms must be conceptually clarified in terms of the POPIA. The first term is 'personal information'.[149] De Hert and Papakonstantinou contend that 'the question, what constitutes "personal data", is evidently critical while establishing whether data protection legislation is applicable.'[150] In terms of the POPIA, personal information is 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person'.[151] The provision provides a non-exhaustive list of personally identifiable information to include non-sensitive information (information relating to sex, gender, and personal opinion) and sensitive information (like information relating to religion, sexual orientation, medical and criminal history).[152] The list does not expressly include internet-related personal data of contemporary relevance such as Internet Protocol (IP) addresses[153] or cookie identifiers, and clickstream data.[154] As mentioned above, however, the list is not exhaustive, and it is submitted that all of this personal information is included provided it can reasonably be linked to an identifiable person.

---

146 South African Constitution, sec 14 which opens with 'everyone'. Compare with section 37 of the Nigeria Constitution.

147 POPIA, sec 3(b)(ii).

148 POPIA, sec 3(b)(ii).

149 Data and information is used interchangeably in this chapter.

150 De Hert & Papakonstantinou (n 102 above)132.

151 POPIA, sec 1.

152 See Roos (n 10 above) 369

153 Bygrave contends that "[o]ne of the most vexed issues in this area [data privacy law] is whether Internet Protocol (IP) addresses may constitute 'personal data'" Bygrave (n 129 above) 137. For more elaborate discussions on the debates regarding IPs and personal information, see Schwartz & Solove (2011)(n 139 above) 1836-1841.

154 According to art 4 of the draft EU Regulation, 'genetic data' 'means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development.' See De Hert & Papakonstantinou's discussion with regard the EU Regulation. (n 104 above) 133.

Two features of the POPIA's definition (of personal information) are insightful. Firstly, the definition, in line with the recent trend in legislating for data privacy, has been broadened in terms of the possibility of identification.[155] This is partly to cope with the fact that 'information can now be connected and harvested through the use of advanced techniques in order to create profiles.'[156] Thus non-identifiable information can be easily made identifiable. The second striking feature of the definition is that it includes personal information on juristic persons, thus making them protected under the Act.[157] This is suggestive of the *sui generis* nature of data privacy.[158] The SALRC was of the opinion that '[j]uristic persons like natural persons are affected by increased processing of information on them thus they should also be protected.'[159] This is not surprising as juristic persons are also entitled to certain rights under the South African Constitution and the common law.[160]

Another key term used in section 3(1) of the POPIA is 'processing'. According to the POPIA, processing 'means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information'.[161] It covers a wide range of activities on personal data including collecting, dissemination and degradation.[162] Roos contends that the "definition is so wide that one can argue that 'processing' could be any action performed on personal information."[163] It is our view that broad definition of processing is also in line with the trend adopted by data privacy law to ensure greater protection for individuals.

---

155 See B Van der Sloot 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4 (4) *International Data Privacy Law* 309 where she argued that right from the CoE Resolution, to the OECD Guideline to the EU Directive and presently, the EU Regulation, a conscious attempt has been made to widen the definition of personal data so as to 'focus [more] on the individual, his interests and his right to control'. 310.

156 Van der Sloot (n 155 above) 310.

157 A Visser & D Strachan 'South Africa' in M Kuschewsky(ed) *Data protection and privacy: Jurisdictional comparisons* (2012) 517. Even Bygrave observes that '[t]he data privacy legislation of the overwhelming majority of countries does not provide express protection for data on collective entities'. By collective entities, he refers to juristic persons. Bygrave (n 129 above) 139.

158 SALRC (n 15 above) para 3.3.38.

159 SALRC (n 15 above) para 3.3.3., para 3.3.41. See also J Neethling 'Data protection and juristic persons' (2008) 71 *Tydskrif vir hedendaagse Romeins-Hollandse Reg (THRHR)* 71. Indeed the SALRC further state a justification for the protection of juristic persons under the POPIA that '[i]f juristic persons were excluded from the application of the proposed data protection measures, credit bureaux, eg, would be in a position to collect and use information on the creditworthiness of companies without any constraints except perhaps those imposed by the totally inadequate traditional common law data protection principles.' SALRC (n 15 above) 3.3.43.

160 South African Constitution, sec 8(3).

161 POPIA, sec 1.

162 POPIA, sec 1.

163 Roos (n 10 above) 368

5.4.2.4. Conditions for the lawful processing of personal information (fair information principles (FIPs))

The FIPs are critical in any data privacy instrument.[164] Their aim is to ensure fair and lawful processing of the personal data of individuals.[165] The POPIA provisions on the FIPs show insight for three reasons. Firstly, the principles form an integral part of the law with very detailed provisions. [166] Secondly, the SALRC has adopted a 'flexible-based principle' regime so as to make the law applicable to 'widely divergent sectors' and 'resilient to rapid and consistent technological developments'.[167] Thirdly, the POPIA recognises contemporary challenges of the internet and has integrated some internet-specific obligations which depict the new generation of data privacy instruments with internet-specific rights and obligations.[168] This is partly an acknowledgement of the enormous threats the internet possesses to data privacy in this computer age.[169] The principles will now be discussed in greater detail.

a. Accountability

Accountability is a relatively new idea in data privacy law.[170] It is used as 'an umbrella concept which covers a myriad of obligations'.[171] Accountability is a condition for lawful processing that requires a responsible party to ensure that all the other conditions (or FIPs) are complied with.[172] The principle further specifies a time for the principles to be complied with. In terms of section 8 of the POPIA, the conditions for the lawful processing of personal data must be present 'at the time of determination of the purpose and means of processing and during the processing itself'.[173] This means compliance with the FIPs cannot be retrospective in any way. For the purpose of proper accountability, a question

---

164 See generally FH Cate 'The failure of fair information practice principles' in JK Win (ed) *Consumer protection in the age of the information Economy* (2006)

165 Roos (n 97 above) 79; perhaps that is a reason why the FIPs are also called "good information handling". See SALRC (n 15 above) para 4.2.13.

166 SALRC (n 15 above) 4.2.23.

167 SALRC (n 15 above) para 4.2.22.

168 Eg, the right to delete or right to be forgotten as discussed below. This is in the line of the draft EU Regulation on data privacy.

169 This is not surprising as South Africa is the most internet connected country in Africa. See Ncube (n 26 above) 345.

170 Accountability is not contained in the EU Directive, but it has been incorporated as one of the innovations in the draft EU Regulation. It is linked to the obligation of transparency in the EU Regulation. See Van der Sloot (n 155 above) 4.

171 See Van der Sloot's discussions with regard the accountability principle under the draft EU Regulation (n 155 above) 7.

172 POPIA, sec 8.

173 POPIA, sec 8.

may be asked regarding the particular official that should be responsible to oversee compliance with the FIPs in an institution. This is because modern data processors are usually very large multinational entities and government departments which comprise of employees with different responsibilities. Section 8 is silent in this regard. It is this researcher's view, however, that accountability is largely the task of the information officer of an organisation.[174] Based on section 1 of the POPIA, an information officer in a government department is 'an information officer or deputy information officer as contemplated in terms of section 1 or 17 of the PAIA.'[175] In a private institution, an information officer is the head of a private institution as contemplated in section 1 of the PAIA.[176] Nevertheless, Roos points out that, although information officers are responsible for supervising the day-to-day compliance with the FIPs in an organisation, 'it is important to note that the "responsible party", and not the information officer, ultimately is the person accountable.'[177]

Accountability mainly reinforces trust in the data processing environment and enables individuals to enforce their rights given that modern day data processing is conducted behind closed doors.[178]

b. Processing limitation

The processing limitation principle 'embraces four aspects limiting the processing of personal information to ensure that processing is done by lawful means.'[179] The first aspect requires that personal information must be lawfully and reasonably processed 'in a manner that does not infringe the privacy of the data subject.'[180] The SALRC pointed out that this requirement is crucial because 'it embraces and generates the other core principles of information protection law'.[181] The requirement of fair and lawful processing is the core essence of data protection law which makes it surprising that it is not made the first principle in the POPIA.[182] Nevertheless, its present position does not undermine its value.

---

174 According to the SALRC, "chief information officer". See SALRC (n 15 above) para 4.2.32.
175 See PAIA (n 100 above).
176 See POPIA, sec 55 & 56.
177 Roos (n 10 above) 380.
178 De Hert & Papakonstantinou (n 104 above) 134.
179 Neethling (n 92 above) 248. See also Roos (n 10 above) 372.
180 POPIA, sec 9.
181 SALRC (n 15 above) para 4.2.28. See also Bygrave (n 129 above) 146; Roos (n 8 above) 483.
182 Eg, it is the first principle in the EU Directive (art 6(1)(a)) and draft EU Regulation (art 5(a)). In the draft EU Regulation, the requirement of fair and lawful processing has been merged with the principle

Questions have even been raised regarding whether the principle needs to be included in the Act. Roos argued that 'it is probably not necessary to spell out lawful processing as a specific data protection principle in an Act.'[183] This is because the whole idea of the FIPs in the first place is to ensure lawful processing. It is our view, however, that its inclusion in the POPIA is in order to bring the Act into harmony with international prescripts on data protection.

The second aspect of the processing limitation principle is minimality. In terms of section 10 of the POPIA, 'personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive'.[184] This requirement states that only necessary information should be processed taking into account the purpose of the processing. The requirement of minimality also relates to the information quality principle in that given the purpose of processing of personal information, the responsible party must ensure that such necessary information processed is of the highest quality especially in terms of accuracy at the time of the processing. Minimality is a standalone principle in the draft EU Regulation.[185] The problem with this requirement is that the terms 'adequate', 'relevant' and 'not excessive' may be susceptible to different interpretations. A simpler approach probably should have been the use of the word 'necessary' which unequivocally shows that the personal information being processed must be necessary for the specified purpose.[186] Any information that is not necessary (not relevant, adequate or in excess) for the specified purpose is irrelevant and therefore its processing is unlawful

A further requirement under the processing limitation principle in terms of the POPIA is consent, justification and objection.[187] According to section 11, personal information may be processed only if: the data subject consents; if processing is necessary for the conclusion or performance of a contract to which the data subject is a party; if processing is necessary for compliance with an obligation imposed by law on the responsible party or to protect the legitimate interest of the data subject; if processing is necessary for the performance of a public duty by a public body; and if processing is necessary for the

---

of transparency. Roos argues that the requirement of 'fair' and 'lawful' processing is superfluous as any processing that is fair will definitely be lawful. Roos (n 8 above) 483.

183 Roos (n 8 above) 483, fn 57.

184 Equivalent of art 6(1)(c) of the EU Directive.

185 POPIA, sec 11.

186 See, generally, discussion with regard the requirement of minimality in SALRC (n 15 above) 172-175.

187 POPIA, sec 11.

pursuit of a legitimate interest of the responsible or a third party.[188] All the requirements under section 11(1) are clear. What seems to be problematic under data privacy law is consent. The POPIA defines consent as 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.'[189] The notion of consent is fundamental to data privacy law as it is the major means by which an individual exercises control over the processing of his /her personal data.[190]

Makulilo identifies two main issues with the consent requirement.[191] Firstly, it is sometimes very difficult to obtain the unequivocal consent of a data subject in real life.[192] One will appreciate the difficulty of getting consent when it is considered with regard to large-scale data processing by SNSs or multinationals which handle the personal data of millions of individuals.[193] Will Facebook or Twitter, for instance, be able to contact each user to obtain consent before processing his/her personal data? What most of these online data processors do is to obtain consent merely by giving notices and requiring simply the ticking of a box. In this regard, Kosta posits that '[w]hen… consent can be expressed by the ticking of a box, there are no safeguards that the data subject has actually read the information that is provided before consenting and there is heated debate as to how consent can be provided in online environments'.[194] Can consent in this circumstance be said to be real? It, therefore, seems that obtaining real consent with regard to SNSs is a 'Sisyphean task'.[195] The POPIA, perhaps in recognition of the difficulty of obtaining real consent, places the burden of proving consent on the responsible party and also acknowledges that consent can always be withdrawn.[196] A second difficulty with consent

188 POPIA, sec 11(1)(a-f).
189 POPIA, sec 1.
190 See Art 29 Data Protection Working Party 'Opinion 15/2011 on the definition of consent' available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (accessed 1 November 2015) 8. See also Makulilo (n 32 above) 166; De Hert & Papakonstantinou (n 104 above) 135.
191 Makulilo (n 32 above) 166. Koops also seriously criticised the consent requirement with regard the EU data protection regime. It was her view that consent is a 'myth' especially for internet-based services as people merely tick consent boxes without either reading or understanding the privacy statements. She further notes that '[a]nother challenge of relying on consent is that convenience and people's limited capacity to make rational decisions prevent people from seriously spending time and intellectual effort on reading the privacy statements of every website, app, or service they use.' B Koops 'The trouble with EU data protection law' (2014) 4(4) *International Data Privacy Law* 251- 252.
192 See Makulilo (n 32 above) 166.
193 Usually, large businesses merely require that a box is ticked as an expression of consent.
194 E Kosta *Consent in European data protection law* (2013)138.
195 Koops (n 191 above) 251.
196 POPIA, sec 11(2)(a & b). Withdrawal of consent can, however, only be exercised if the lawfulness of the processing before such withdrawal or processing in terms of sec 1(b)-(f) will not be affected.

is that it is usually subjected to multiple exceptions, especially for security and law enforcement purposes.[197]

The SALRC has, however, pointed out that the POPIA, like several other international data privacy laws, is not 'consent driven'.[198] There are several other alternatives provided in section 11(1)[199] that could be resorted to to legitimise data processing by responsible parties.[200] Finally, POPIA grants a data subject the right to object to the processing of his/her personal data.[201] If the data subject objects on reasonable grounds, the responsible party may cease the processing.[202] In this regard, the stoppage of the processing is not absolute especially when the processing is with respect to instances like: the performance or conclusion of a contract with the data subject; or based on the grounds of protecting the legitimate interest of the responsible party or a third party; or to comply with a public law duty. In these cases, it appears that the data subject may not successfully object on reasonable grounds because his/her interest has to be balanced against other interests. It submitted, however, that the interest of the data subject to control his personal information must be given topmost priority because the section appears to give the responsible party much discretion over the processing of personal information. This contention is held based on the use of the phrase 'may no longer process' in the section 11(4). The EU Directive provides a narrower requirement regarding the right to object. It states that '[w]here there is a justified objection, the processing instigated by the controller may no longer involve [only] those data [objected to]'.[203]

The last limitation under the processing limitation principle is that of direct collection from a data subject. In terms of the POPIA, personal information must be collected directly from the data subject.[204] The provision is, however, subject to several exceptions largely for public and legitimate interest purposes.[205] This requirement is crucial, as it is one of the ways a data subject is acquainted with the processing of his/her personal data.[206]

197 Makulilo (n 32 above) 166.
198 SALRC (n 15 above) para 4.2.93.
199 POPIA, subsecs b-f specifically.
200 SALRC (n 15 above) para 4.2.93.
201 POPIA, sec 11(3).
202 POPIA, sec 11(4).
203 EU Directive, art 14 (a)
204 POPIA, sec 12.
205 POPIA, sec 12 generally.
206 Roos (n 10 above) 374.

c. Purpose specification

The purpose specification principle determines the scope of data processing; it, thus, 'underpins every other aspect of the processing of information'.[207] The first rule with regard to the purpose specification principle is collection for specific purpose. In terms of the POPIA, the collection of personal information must be for a 'specific, explicitly defined and lawful purpose' which relates to the function or activity of the responsible party only.[208] The rule in this principle is applicable to the collection of personal data only since it is, in most cases, the first stage in the data processing operation. Data processing must, thus, be done only for a clearly defined purpose based on the statutory mandate of a government department and in the line of business of a private commercial entity. It goes without saying that the statutory framework for a public agency determines the purpose for the collection of personal information. Such a government department must not collect personal data outside its defined mandate or it amounts to unlawful collection. Determining the purpose of collection for a private entity is tricky as private entities do not operate based on statutory mandates. It is the view of this researcher that the memorandum and articles of association of a private entity should provide a guide to determining the scope of the processing of personal data. Nevertheless, more difficulties arise with regard to processing of other information that do not relate to the purpose of the company such as the processing of its employees personal information. In this respect still, it is submitted that such information must be for the purpose of actualisation of the general objective of the institution which must be clearly spelt out to the relevant party

The purpose specification principle further places an obligation on the responsible party to take appropriate steps to ensure that the data subject is aware of the processing, subject to certain limitations.[209] This requirement goes alongside the openness principle in section 18 which requires that the data subject be notified when his/her personal information is to be collected. It is, therefore, difficult to understand why it needs to be specifically set out separately from the openness principle. The SALRC, however, stated that this is an example of a situation where principles need to be read together.[210]

---

207 Neethling (n 92 above) 250. See also SALRC (n 15 above) para 4.2.131.
208 POPIA, sec 13.
209 POPIA, secs 13(2) &18(4).
210 SALRC (n 15 above) para 4.2.129.

Retention and restriction of records is another aspect of the purpose specification principle. In terms of section 14(1), 'records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed'.[211] This rule is subject to some exceptions, which include retention authorised by law and whether the responsible party reasonably requires the record for lawful purposes.[212] Records may be retained for a longer period in terms of the provision for historical, statistical and research purposes.[213] Also, if the responsible party has used the record to make a decision on the data subject, such a record could be retained for a certain period.[214] If the responsible party is no longer authorised to retain the record, such a record must be destroyed, deleted, or de-identified.[215]

d. Further processing limitation

This condition directly relates to the purpose specification principle, and it requires that further processing of personal information must be 'in accordance or compatible' with the specified purpose under section 13.[216] The SALRC pointed out that 'further processing includes both use and disclosure of information'.[217] Unlike the principle in section 13 (collection for specified purpose only), therefore, this principle is more applicable for the use and disclosure of personal information. This principle largely provides rules for secondary use of personal data, and it is a condition that is easily susceptible to abuse by responsible parties. Determining the level of connection between the specified processing and subsequent processing may appear to be problematic. Responsible parties may hide under this principle to process personal information unlawfully and argue that such processing is 'compatible' with the specified purpose. This is so because it is the responsible party alone who determines what is 'compatible' and what is not, and it is left for individuals to challenge such decision.[218] The POPIA, in a bid to avoid such abuses by responsible parties, expressly outlines specific guidelines to determine whether further processing is compatible with the purpose of collection.[219] A responsible party must take

---

211 POPIA, sec 14(1).
212 See generally POPIA, sec 14(1)(a)-(d).
213 POPIA, sec 14(2).
214 POPIA, sec 14(3). For a reasonable period of time as prescribed by a law or code of conduct.
215 POPIA, sec 14(4). de-identification of personal data has been defined in sec 1 of the POPIA
216 POPIA, sec15.
217 SALRC (n 15 above) para 4.2.174.
218 See De Hert & Papakonstantinou (n 104 above) 135. Their discussion is with respect to the draft EU Regulation with similar provision.
219 POPIA, sec 15(2).

into account the relationship between: processing; nature of the information concerned; consequence of intended further processing; etc.[220] The POPIA also stipulates instances where further processing is compatible with the specified purpose.[221]

e. Information quality

Section 16 of the POPIA provides for the information quality principle. In terms of the Act, a responsible party must ensure that personal information being processed is 'complete, accurate, not misleading and updated'.[222] The essence of this principle is to prevent presenting misleading information about an individual which may lead to loss of benefits or discrimination.[223] Thus, the principle admits of no exceptions.[224] It is submitted that this principle places a very heavy obligation on a responsible party,[225] although Roos argues that the obligation of the responsible party in this regard is not absolute.[226] According to the her, 'the responsible party need only to take "practical steps" to ensure accuracy, taking into account the purpose for which information is collected or subsequently processed.'[227]

f. Openness

The SALRC is of the opinion that the openness principle is the 'the first part of the principle giving effect to data subject participation and control.'[228] Openness relates to transparency, which is one of the cruxes of data privacy law.[229] This principle is crucial given that contemporary data processing is often remotely carried out behind invisible closed doors online.[230] It is, therefore, important that a data subject have knowledge that his/her personal data is being processed. Thus, it was observed that 'even the comprehensive measures for protecting information are worthless if the individual does not

220 POPIA, sec 15(2).
221 POPIA, sec 15(3). Eg where there is consent, where personal data is available in a public record and where further processing is required by law.
222 POPIA, sec 16.
223 See Neethling (n 92 above) 251-252.
224 Roos (n 10 above) 376.
225 Even the SALRC acknowledged the cost implication of this principle on businesses. See SALRC (n 15 above) 4.2.195-7
226 Roos (n 10 above)377.
227 Roos (n 10 above)377. See also POPIA, sec 16(2).
228 SALRC (n 15 above) 4.2.198.
229 See generally P De Hert & S Gutwirth 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes *et al Privacy and the criminal law* (2006) 61-104.
230 Probably in clouds and databases.

have such knowledge.'[231] The first part of this principle requires that a responsible party must document all data processing activities based on the PAIA.[232] The reason for proper documentation is to enable data subjects to have access to their personal data.

The second part, which is strikingly similar to section 13(2), obliges the responsible party to notify the data subject when collecting personal information.[233] Thus, if personal information is collected, the responsible party must 'take reasonable practical steps' to ensure the data subject is aware of details of the personal information collected by the responsible party.[234] Section 18(2) specifies a timeframe within which the data subject should be informed.[235] The requirement of notifying each data subject before collecting his/her personal data seems to be the most onerous among the obligations of the responsible party. This is particularly so for large data processors (responsible parties) like Microsoft and Apple. These data processors will be required to contact each of their users to notify them of data processing. In fact, it may even be bothersome for data subjects to have to be communicated by each responsible party in possession of their personal information.[236] This may have been possible years back where data controllers and data processing were extremely limited, but not in the current, increasingly ubiquitous computing environment. [237] Responsible parties have found a way round this requirement merely by putting notices about data processing on their websites. The question, however, remains as to whether this form of notification is sufficient given that consumers rarely read them.[238] The EU Commission is trying to initiate reforms in this area as the requirement of notification has been replaced with documentation in the draft EU Regulation.[239] The POPIA provides for documentation which makes it surprising to see that it still retains the antiquated notification requirement despite the cost implications on

---

231 SALRC (n 15 above) 4.2.199.

232 POPIA, sec 17. Documentation as required in the principle should be as referred to in sec 14 to 51 of PAIA. Sec 18(1) is, however, subject to some exceptions provided in subsec 4. Thus compliance with the sec is not necessary if: there is consent; non-compliance will not prejudice the data subject's interest; and for other legitimate public purposes.

233 POPIA, sec 18.

234 An extensive list of the details is provided in sec 18(1).

235 Based on sec 18(2), if the information is collected directly from the data subject, he/she must be informed before collection or else as soon as practicable after collection.

236 Imagine having to be communicated with by each entity in possession of one's personal information, such as SNSs and several other service providers!

237 De Hert & Papakonstatinou (n 104 above) 139.

238 See Roos (n 30 above) 401 where she observes that people hardly read privacy policies.

239 See van der Sloot (n 155 above) 7-8. She contends that the EU has shifted to a more risk focused processing. The EU Directive does not provide for this kind of notification. Based on art 18, notification is required to be made only to the supervisory authority in cases of automated processing.

responsible parties.[240] The first draft of the POPIA requires that the responsible party must notify the Regulator[241] in addition to notifying the data subject[242] before processing (in this case collection). The obligation to notify the Regulator has been removed from the present Act – there is only a requirement to notify the data subject. It is the view of this researcher that notifying the Regulator before processing personal information is also a very onerous responsibility. In fact, the feasibility of notifying both individuals and the Regulator is doubtful considering the increasingly ubiquitous nature of information processing nowadays. Information processing is no longer carried out by identifiable data processors in a particular place but through the internet with ubiquitous services like clouds. The approach of documentation, it is submitted, appears more relatively realistic. The approach can also be supported by the role of a proactive DPA and conscious data subjects.

The openness principle is not known to the South African common law of delict which is one of the shortfalls of the common law with regard to data privacy protection.[243]

g. Security safeguards

This principle is better appreciated when considered with respect to numerous high-profile data breach cases recently.[244] In addition, the rising spate of identity thefts and cybercrimes in sub-Saharan Africa makes this principle crucial to African states. This principle is divided into certain major parts with each part placing specific obligations on responsible parties. The first part of the principle is on security measures for the integrity and confidentiality of personal information. In terms of section 19(1) of the POPIA, responsible parties must secure the integrity and confidentiality of personal information in its possession or under its control. This should be done by taking appropriate, reasonable, technical and organisational measures to prevent loss or damage and unlawful access of personal information.[245] Technical measures may involve the use of technologies to enhance the security of personal data in the databases of responsible parties. These technologies are in the form of software to prevent unauthorised access, generically called

240 It is indeed costly for business to have to contact each data subject whenever it wants to process his/her personal information.

241 Sec (16)(1) of the first draft of the Personal Information Protection Bill is available at http://www.dcs.gov.za/homepage_paia/Documents/Legislation/Bill-draft-privacy.pdf (accessed 1 November 2015)

242 (n 241 above), sec 16(2).

243 Neethling (n 92 above) 252.

244 See D Morley *Understanding computers in a changing society* (2015) 142. See also D Morley & C Parker *Understanding computers: Today and tomorrow* (2013) 346.

245 POPIA, sec 19 (1)(a) &(b).

privacy enhancing technologies (PETs).[246] They include: automatic anonymisation after a certain period of time; encryption tools; cookie-cutters; the platform for privacy preferences (P3P).[247] This principle, therefore, upholds Lessig's theory on the regulation of data processing.[248] Indeed, even the SALRC was 'in full support of the use of new technologies that enhance the security of personal information especially in so far as they promote the principles of minimality or de-identification.'[249] The POPIA's approach in this regard shows insight as it depicts a paradigm-shift in data privacy law-making.[250]

The second part of the safeguard principle requires an operator, or anyone processing personal information on behalf of a responsible party, to do so only with the knowledge and authorisation of the responsible party.[251] The operator must treat information which comes to his/her knowledge as confidential.[252] It is, however, unclear from this requirement whether the operator will be liable for the failure to comply with the provisions of the POPIA or whether the responsibility party is vicariously liable. The latter seems to be more probable. This is because section 21 requires the responsible party to use a written contract with the operator to ensure that 'the operator…maintains the security measures' provided in section 19.[253]

To further enhance the security of personal information under the control of a responsible party, an obligation to notify the Regulator and the data subject (in certain cases)[254] 'where there are reasonable grounds to believe that personal information…has been accessed or acquired by any unauthorised person' is established by this principle.[255] This obligation,

246 Or through the use of privacy by design (PbD) as discussed in chapter 2.

247 See European Commission 'Privacy enhancing technologies (PETs): The existing legal framework' available at http://europa.eu/rapid/press-release_MEMO-07-159_en.htm (accessed 1 November 2015).

248 Lessig's theory has been elaborately discussed in chapter 2.

249 SALRC (n 15 above) para 4.2.281.

250 Protecting data privacy by the use of technologies is also one of the topics of discussion under the draft EU Regulation. See European Commission Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions 'A comprehensive approach on personal data protection in the European Union' available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (accessed 1 November 2015)12.

251 POPIA, sec 20.

252 POPIA, sec 20.

253 POPIA, sec 21.

254 In terms of sec 22(3), the responsible party may delay notification to the data subject if such notification will impede criminal investigation in terms of the provision.

255 POPIA, sec 22(1). This is also one of the innovations of the draft EU regulation.

usually called data breach notification, is also one of the new features of data privacy legislation.[256]

h. Data subjects' participation

This principle follows from the openness principle and it gives data subjects active control over the processing of their personal data. It grants data subjects the right to play a more active role in the processing of their personal information. The principle confers two major rights on a data subject. The first, in terms of section 23, is the right to access personal information having provided adequate proof of identity.[257] It is our view that this right appears to be a duplication of the openness principle. A line of distinction may, however, be drawn between both. While the openness principle merely obliges the responsible party to ensure that the data subject has knowledge of the processing of his/her personal information, the right of access under the data subject participation principle grants a data subject the right to access and view such personal information. Thus, a data subject must take positive steps to enjoy this right.

The second right based on the data subject participation principle is the right to correction of personal information. In terms of section 24, the data subject can request a responsible party to 'correct or delete' information which is 'inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully'.[258] The data subject may also request that the personal information of a responsible party he/she is no longer authorised to retain should be destroyed or deleted in terms of section 14.[259] This principle, therefore, shows how the full powers granted to the data subject in terms of the POPIA can be exercised.

i. Processing of special sensitive information and personal information about children

The regime on sensitive data processing is not part of the FIPs, but discussions on it can take place under this part. The processing of sensitive personal information is, generally

256 See draft EU Regulation, arts 31 & 32. For more on data breach notification under in the EU, see generally R Wong *Data security breaches and privacy in Europe* (2013).
257 POPIA, sec 23.
258 POPIA, sec 24 (1)(a).
259 POPIA, sec 24(1)(b).

prohibited under the POPIA.[260] In terms of section 26, a responsible party is generally prohibited from processing personal information relating to religious or philosophical beliefs, race or ethnicity, trade union membership, political persuasion, health, sex life, biometric information and criminal behaviour.[261] In the usual style of the POPIA, specific exceptions are provided for where sensitive data or special personal information can be lawfully processed.[262] In terms of section 26, special personal information can be processed if: the data subject consents; processing is necessary for the establishment of a right or obligation; the processing is necessary to comply with an obligation under international law; the processing is for historical and statistical research purpose;[263] the information is deliberately made public by the data subject; and other more specific exceptions in terms of section 28-33 of the POPIA. Similarly, the processing of children's personal information is prohibited as provided in section 34. This requirement is also subject to specific exceptions.[264]

By the prohibition of the processing of special personal data, the POPIA adopts the style in the EU Directive and draft EU Regulation. The POPIA, however, does not include genetic data as part of sensitive personal data.[265] Another problem with the provision on sensitive data processing is that processing-intensive methods have blurred the distinction between sensitive and non-sensitive data.[266] Processing of non-sensitive data, like a person's name, can lead to the discovery of sensitive information such as religious or ethnic affiliations. Bernal holds a similar view when he pointed out that, '[t]he developing techniques of data

---

260 Except where there is explicit consent. See SALRC (n 15 above) para 4.2.93. The provision on sensitive personal information is, *ab initio,* couched in the negative based on sec 26 which provides that: 'A responsible party *may […] not* process personal information' that is considered sensitive. This provision is slightly different with regard to all other personal information which are not sensitive as sec 11 (1) provides that 'personal information *may only be* processed if…' [Emphasis added]. In this case, the latter sec is couched in a permissive way.

261 To the extent that such information relates to alleged commission by a data subject of any offence or any proceeding in respect of alleged commission of crime. POPIA, sec 26(b). See generally sec 26.

262 POPIA, sec 27.

263 In terms of the POPIA, such historical and statistical research purpose must serve the public interest, the processing is necessary as such, and it will be impossible or difficult to obtain consent. See POPIA, sec 27(1)(d).

264 POPIA, sec 35(1)(a) – (f). largely based on consent of a competent person to act instead of the child; necessity to establish a right or legal obligation; comply with an obligation of international public law, historical, statistical or research purpose and information deliberately being made public by the child with consent of a competent person.

265 This was is included in the draft EU Regulation. See De Hert & Papakonstantinou (n 104 above)133.

266 As identified by De Hert & Papakonstantinou (n 104 above) 133 (with respect to the draft EU Regulation). See also R Wong 'Data protection online: Alternative approaches to sensitive data? (2007) 2(1) *Journal of International Commercial Law and Technology* 9-16. In this article, the author analysed two main approaches to sensitive data protection i.e. 'purpose-based approach' and 'contextualised - approach.'

aggregation and profiling means that non-sensitive data also needs to be considered much more carefully.'[267] It is thus left for the Regulator and the court to be cautious when dealing with issues of this nature.

5.4.2.5. Rights of data subjects

Section 5 of the POPIA outlines all the rights of a data subject and, by implication, the duties of a responsible party which run throughout the entire Act. A data subject or responsible party does not need to go through all the provisions of the Act before he/she knows what rights he/she has with respect to the processing of his/her personal information. It is our view that the POPIA, by delineating the rights in the initial part, has shown that the Act focuses to a larger extent on the human rights of individuals. This approach is a useful lesson for countries with a low-level of awareness on data privacy issues.

In terms of section 5, '[a] data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3'.[268] This right includes the right to: be notified of the processing of his/her personal information; establish whether a responsible party holds his/her personal data and to request access to such personal information; request the correction, destruction or deletion of personal information; and object to the particular processing of personal information. Other rights include: the right to object to the processing of personal data for direct marketing purpose; not to have personal information processed for direct marketing by means of unsolicited electronic communications; not to be subjected to any decision based on the automated processing of personal data; to submit a complaint to the Regulator on interference with protection of personal information. Similarly, a data subject has the right to institute civil proceeding regarding alleged interference with the processing of his/her personal information. All these rights are to be exercised in terms of well-defined conditions specified in chapter 3 of the Act and subject to specific exceptions.

---

267 PA Bernal 'The right to delete?' 2011 2(2) *European Journal of Law and Technology.* Also available at http://ejlt.org/article/view/75/144#_edn7 (accessed 1 November 2015).

268 POPIA, sec 5.

5.4.2.6. Exceptions, exemptions and exclusions

The terms 'exceptions', 'exemptions' and 'exclusions' may be confusing when used in a law. The SALRC provides guidance on the application of each term in the POPIA. Exceptions to the FIPs define their limits as very few principles are absolute.[269] The exceptions limit the rule in the FIPs and 'map out the extent of the obligations under the rule (or principle)'.[270] Most of the principles discussed above have specific exceptions which go with the rule itself. 'The exceptions are identical in several of the principles. Others appear in one principle but not another.'[271] On the other hand, exemption 'involves lifting a burdensome obligation from a responsible party while the burden continues to apply to others.'[272] Thus, exemptions do not affect the FIPs but merely exclude certain responsible parties from the Act's provision. Exclusions are similar to exemptions, however, in the former (exclusions), *certain classes of responsible parties* are totally excluded from the scope of the Act.[273] The main difference between exemption and exclusion is the range of responsible parties covered.

Section 6 provides for exclusions. In terms of the provision, the Act does not apply to the processing of information: in the course of a purely personal or household activity; that has been de-identified; by a public body for the purpose of national security or prevention and detection of crime; by cabinet members and its committees; or the executive council of a province; and relating to judicial functions of a court as specified in section 166 of the constitution.[274] The underlying philosophy of these exemptions and exclusions is that the threat to data privacy is either too small (*de minimis)* or other interests override the data privacy right of the data subject.[275]

Two of the above listed exclusions deserve further comment. With respect to exclusion for purely personal or household activity, Roos argues that this category of processing does not create a serious threat to privacy infringement.[276] She contends further that this exception applies only 'as long as the individual collecting the information does not place

269 SALRC (n 15 above) para 4.4.3.
270 SALRC (n 15 above) para 4.4.3.
271 SALRC (n 15 above) para 4.4.3.
272 SALRC (n 15 above) para 4.4.3.
273 SALRC (n 15 above) para 4.4.3.
274 See POPIA, sec 6(1).
275 SALRC (n 15 above) para 4.4.4.
276 Roos (n 97 above) 79. The discussion is with respect to the New Zealand Privacy Act of 1993.

it on the internet and make it available to more persons than his or her family!'[277] With respect to exclusion as a result of de-identification, the difficulty of realising absolute anonymisation in practice has been discussed several times.[278] Bernal contends that:

> …it must be remembered that anonymisation is far from a reliable process. Indeed, there is evidence to suggest that much supposedly 'anonymised' data can be 'de-anonymised', by combining it with other, often public, data sources.[279]

For the processing of personal information for journalistic, literary or artistic purposes, the POPIA does not apply 'only to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right of privacy with the right to freedom of expression.'[280] This section is couched in a narrow way so, if processing is not necessary to reconcile privacy with freedom of expression, the conditions for lawful processing in section 3 still apply. The POPIA also provides for where a responsible party who processes personal information for journalistic purposes is subject to a code of ethics which provides an adequate safeguard by virtue of his office, employment or profession. In such instances, the code will apply and not the POPIA.[281]

With regard to exemptions, chapter 4 of the POPIA provides certain situations where the Regulator is empowered to exempt some responsible parties from the FIPs. The SALRC was of the view that '[s]tatutory exemptions from particular principles are to be preferred over exclusion from the Act of an entire class of responsible party or information.'[282] The Regulator may, thus, exempt certain responsible parties from the conditions for lawful processing if the Regulator is satisfied that public interest outweighs interference with privacy or the processing 'involves a clear benefit to the data subject or third party' that outweighs interference with privacy.[283] Millard states that authorizing

277 Roos (n 97 above) 79.

278 Eg, the EU Commission stated in a recent report that '…we believe that the serious problems stemming from the near-impossibility of full anonymization [or de-identification] of personal data in the new socio-technical global environment pose some of the most crucial challenges to data protection, and should be at the heart of any debate on a review of the European data protection regime.' See European Commission Directorate-General Justice, Freedom and Security 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological development' Final report available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf (accessed 1 November 2015) 48.

279 Bernal (n 267 above).

280 POPIA, sec 7(1).

281 POPIA, sec 6(2). subsec 3 gives guidance in cases of dispute regarding adequacy of such code.

282 SALRC (n 15 above) para 4.4.2.

283 POPIA, sec 37.

processing based on this exemption is a complicated matter especially with respect to financial service providers who offer services, such as medical aid schemes and insurance (like life insurance schemes). He contends further that 'whether a financial product is indeed beneficial is a question of fact and as it is not possible to know all the facts in advance'.[284] It is submitted that this provision grants the Regulator a wide discretion which must be exercised cautiously. Processing in accordance with section 38 is also generally exempted.[285]

5.4.2.7. Regime of transborder data flow

Section 72 of the POPIA prohibits a responsible party from transferring personal information of a data subject to a third party outside South Africa. Certain exceptions are, however, provided in the provision. The first exception is if the third party is 'subject to a law, binding corporate rule or binding agreement which provides *an adequate level of protection'*. Determining an adequate level of protection may be problematic. The POPIA has, however, given guidance in this regard. According to the Act, such law, binding corporate rule or agreement must uphold principles which are *substantially similar* to the conditions for the lawful processing of personal information relating to a data subject'.[286] Also, the law, binding corporate rule or binding agreement must include provisions *substantially similar* to section 72 (on the transfer of personal information outside the Republic). Section 72(1) is problematic because it does not provide for the machinery to assess an adequate level of protection in a foreign country.[287] It is arguable that the Regulator will be empowered to determine adequacy. It may, however, be too early to make such insinuations as the determination of adequacy is not among the functions of the Regulator stipulated in the Act.[288] This is indeed, a serious shortcoming of the POPIA which must be subsequently looked into. The second problem with section 72(1) is that it does not specify which country's 'conditions for the lawful processing of personal information' is being referred to. As trivial as this omission may seem, it is significant

---

284 Millard (n 21 above) 618.

285 Sec 38 relates to personal information processed for the purpose of discharging a relevant function. Relevant function means any function of a public body or conferred in terms of the law which is performed with the view to protecting members of the public against financial loss due to fraud.

286 POPIA, sec 72(a)(i).

287 Unlike the EU that has provided for extensive adequacy assessment mechanism in terms of art 25 and 26 of the EU Directive.

288 See POPIA, sec 40.

because the provision refers not only to South Africa but a 'foreign country'.[289] The first draft of the POPIA has a clearer provision in this regard. The draft Bill provides in section 94(a) that personal information may only be transferred to a responsible party in a foreign country who is subject to 'a law…[that] upholds principles for fair handling of the information that are substantially *similar to the Information Protection Principles set out in Chapter 3 of this Act.*'[290]

The regime of transborder data flow in South Africa came under heavy criticism in the discussions preparatory to the Act.[291] A very insightful argument against the provision was that it will affect South African's relations with other African states. It was contended that:

> [t]he majority of African States, if not all, have no information privacy legislation in place and subjectively it is foreseen that with the problems of the continent being what they are, the introduction of such legislation will not be seen for some considerable time. South Africa is presently increasing its presence on the continent and many South African organisations have offices throughout Africa. In effect this will mean that South Africa would isolate itself from the rest of the continent in its attempt to blindly follow directives designed for economies far removed from Africa and South Africa.[292]

Because of the strong desire to have South Africa satisfy the adequacy requirement of the EU, the provision was still incorporated. Several exceptions are, however, provided where transfer to a third party in a foreign jurisdiction can be effected.[293] These exceptions include where the data subject consents, where transfer is necessary for the conclusion or performance contract between a data subject and responsible party or necessary for the conclusion or performance of a contract in the interest of the data subject.[294]

---

289 Sec 72(1) provides that personal information about a data subject many not be transferred to a third party in a *foreign country* unless 'the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that- (i) effectively upholds principles for reasonable processing of the information *that are substantially similar to the conditions for the lawful processing of personal information* relating to a data subject who is a natural person and, where applicable, a juristic person…' [Emphasis added]

290 (Emphasis added).

291 SALRC (n 15 above) 420-423.

292 SALRC (n 15 above) 422-423.

293 POPIA, sec 72(1)(b-e).

294 POPIA, sec 72(1)(b-e).

5.5. An analysis of the (proposed) oversight and enforcement structure of data privacy law in South Africa

The Information Regulator and the court[295] are the primary oversight and enforcement institutions of data privacy law in South Africa based on the POPIA's regime. The analysis in this part will, therefore, focus on these institutions.

5.5.1. The Information Regulator

Section 39 of the POPIA establishes the Information Regulator as the primary enforcement agency for data privacy right in South Africa. The Information Regulator is an independent juristic person with jurisdiction throughout South Africa.[296] It operates in a 'commission-like structure' rather than as an independent regulator.[297] The Regulator is responsible for enforcing the POPIA and PAIA.[298]

It has been pointed out that a Data Protection Authority (DPA), irrespective of the jurisdiction, is supposed to play seven key roles for the realisation of the right to data privacy. They are the roles of an ombudsman, auditor, consultant, educator, policy advisor, negotiator, enforcer and international ambassador.[299] This section analyses the scope of the powers of the Information Regulator with a view to determining the extent to which these roles are provided for in the POPIA.

The role of an **educator** is the first duty and function of the Information Regulator provided in the POPIA. This, in this researcher's view, depicts the importance of this role given the low level of awareness of data privacy issues in African countries generally. Thus, the Information Regulator is to provide education by: promoting understanding of the conditions for lawful processing; undertaking education programmes; making public

---

295 Although the data subject has the powers to sue the responsible party, such action will not be considered as an independent enforcement action since such actions still fall within the general powers of the courts.

296 POPIA, sec 39 generally.

297 SALRC (n 15 above), para 7.2.192. The advantages of the commission-like structure over an independent regulator as identified by the SALRC are: it '[h]elps reduce the danger that regulators will feel vulnerable and behave defensively; creates the sense that decisions follow internal debate; increases legitimacy and accountability; and spreads the workload involved in regulating complex industries.' See SALRC (n 15 above) para7.2.115.

298 POPIA, sec 39(c).

299 See CJ Bennett 'The Office of the Privacy Commissioner of Canada: Regulator, educator, consultant and judge'. Paper presented at conference on "Two sides of the coin: Relations between parliamentary agencies and the public service." Canadian centre for management development, March 2002. See also SALRC (n 15 above) para 7.2.24.

statements; and giving advice to data subjects on data privacy issues.[300] All of these specific roles show insight as they reveal how a greater awareness of data privacy issues can generally be improved in a country.

As an **enforcer** and **policy adviser**, the Information Regulator monitors and enforces compliance with the Act; undertakes research into information processing and computer development and reports the results to the minister; examines proposed legislation or government policy that may affect data privacy right; reports to parliament on data privacy issues; and conducts assessment on data processing.[301] The Regulator also has the duty to issue codes of conduct and make guidelines.[302]

As an **auditor**, the Information Regulator is to be proactive in preventing data privacy violation before it occurs. Thus, the SALRC recommended that the Regulator should 'be empowered to act pro-actively to identify and resolve systemic issues before a breach occurs'.[303] A contemporary proactive role of the data privacy enforcement body is to conduct a privacy impact assessment. This role is manifestly missing in the POPIA; the information Regulator is, however, empowered to conduct an 'assessment … of a public or private body, in respect of the processing of personal information by that body for the purpose of ascertaining whether or not the information is processed according to the conditions for lawful processing of personal information.'[304]

The Information Regulator also plays the role of an **international ambassador**[305] by 'co-operating on a national and international basis with other persons and bodies concerned with the protection of personal information.'[306] Thus, the Information Regulator is 'to facilitate cross-border cooperation in the enforcement of privacy laws by participating in any initiative that is aimed at bringing such cooperation.'[307] The Information Regulator is also 'to conduct research and report to the parliament from time to time on the desirability

---

300 POPIA, sec 40(1)(a).
301 POPIA, sec 40(1)(b).
302 POPIA, sec 40(1)(f).
303 SALRC (n 15 above) para 7.2.191.
304 POPIA, sec 40(b)(vi); see also secs 89-91.
305 The negotiator role can also fit into the role of an international ambassador. The Oxford Advanced Learners Dictionary defines a negotiator as 'a person who is involved in formal political or financial discussions, especially because it is their job.' See Oxford Advanced Learners Dictionary available at http://www.oxfordlearnersdictionaries.com/definition/english/negotiator?q=negotiator (accessed 1 November 2015).
306 POPIA, sec 40(1)(c).
307 POPIA, sec 40(1)(g).

of acceptance, by South Africa, of any international instrument relating to protection of personal information'.[308]

The role of an **ombudsman**[309] seems to be the most crucial among the roles of the Information Regulator. This role is further strengthened by the role of the enforcer. In terms of the Act, the Regulator is to handle complaints: by receiving and investigating complaints on violations of personal information of data subjects; by gathering information that will assist in carrying out its function under the Act; by attempting to resolve complaints by alternative dispute resolution mechanism; and by serving notices in terms of the Act.[310] Thus, any person can submit a complaint alleging 'interference with (the) protection of personal information of (a) data subject'.[311] Such a complaint must be in writing.[312] On receipt of the complaint, the Regulator may: conduct a pre-investigation; act as a conciliator or decide not to take any action;[313] conduct a full investigation or refer the complaint to the enforcement committee.[314] The Regulator must thereafter inform the complainant and responsible party of the course of action taken.[315] If the Regulator decides to investigate, he has a large range of powers at its disposal for the purpose of investigation which include summons, administering an oath, the receipt and acceptance of evidence.[316] The Regulator cannot, however, issue a warrant.[317] After the completion of an investigation, the Regulator may refer the matter to the enforcement committee for consideration.[318] After considering the recommendations of the enforcement committee, the Regulator may issue an enforcement notice requiring a responsible party to take certain steps within a time frame or refrain from taking such steps or to stop the processing of the information specified in the notice.[319]

---

308 POPIA, sec 40(1)(e)(i).
309 This role also relates to the role of the negotiator.
310 POPIA, sec 40(1)(d).
311 As defined in sec 73.
312 POPIA, sec 75.
313 Largely based on conditions in sec 77 which include lapse of times; trivial, frivolous and vexations complaint.
314 POPIA, sec 76(1)(d).
315 POPIA, sec 76(2).
316 POPIA, sec 81.
317 The Regulator must approach a judge of a High Court, a regional magistrate or magistrate in terms of sec 82.
318 POPIA, sec 92.
319 POPIA, sec 95.

5.5.2 The Courts

A responsible party, having been served with notice (information or enforcement), may 'appeal to the High Court having jurisdiction for setting aside or variation of the notice.'[320] A complainant also has the right to appeal in certain circumstance to the High Court having jurisdiction.[321] On appeal, if the court finds that the decision or notice brought before it is not in accordance with the law or notice, or the decision involved an exercise of discretion by the Regulator that ought to have been exercised differently, the court may set aside or substitute the notice or decision.[322] A data subject or the Regulator (if requested) may also bring a civil action for damages in court for breach of provisions in the Act referred to in section 73.[323]

The role of the court in data privacy enforcement appears to be limited. In addition, the exact nature of the relationship between the Regulator and the court is uncertain. Questions could arise regarding whether a data subject can jettison the Regulator and approach the court directly in cases of breach of the provisions of the POPIA. It is submitted that nothing in the Act suggests otherwise, as even section 5, which lists the rights of the data subject, mentions both submission of a complaint to a Regulator and the court as independent rights. Furthermore, based on section 34 of the South African Constitution, a data subject can approach the court directly.[324] A data subject may also allege violation of his/her (data) privacy and bring an action for the enforcement of his/her right under section 38 of the Constitution since the POPIA declares that its purpose to 'give effect to the constitutional right to privacy'.[325] If the earlier view in this regard is taken as the correct position of the law, it may significantly reduce the role of the Regulator in data privacy protection. The point must however be stressed that people do not like to approach the courts directly due to the expenses and time wastage involved.

---

320 POPIA, 97(1).
321 POPIA, sec 97(2).
322 POPIA, sec 98/
323 POPIA, sec 99. Sec 33 relates to breach of conditions of lawful processing in chapter 3 and non-compliance with certain provisions of the Act.
324 South African Constitution, sec 34 provides that 'everyone has the right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum.'
325 POPIA, sec 2(a).

5.6. Insights from selected topic areas in the POPIA

It is important specifically to set out certain focus areas which generate considerable debate on data privacy worldwide and their applicability under the POPIA. This is essential so as to enable policymakers considering a data privacy framework to formulate a law which will be in line with international prescripts. Three topic areas in the POPIA are, thus, selected.

5.6.1. Direct marketing and unsolicited electronic communication (spam)

The legal implication of direct marketing and spam has over time generated considerable debate in the field of data privacy law. Direct marketing is a marketing strategy where the marketer communicates directly with a customer for the purpose of promoting goods or services and which is directed at particular individuals or customers.[326] The communication between the marketer and the customer is carried out by various means, ranging from mail to telephone and fax. With advances in technology, however, and the growth of e-commerce, the internet has taken over as a major medium for direct marketing. For the success of direct marketing, marketers need to address specially targeted audiences and this can be done only through their personal information.[327] Although, direct marketing and spam overlap in some respects; certain differences can, however, be maintained between both.[328] Hamann and Papadopoulos consider that 'spam is a wider expression than direct marketing and therefore it is important to keep in mind that not all direct marketing is spam and not all spam is direct marketing.'[329] Spam is the sending of unsolicited commercial messages (mostly via email or other electronic means) to 'individuals with whom the mailer has had no previous contact and whose contact details are mostly collected from the public spaces of the internet newsgroups, mailing lists, directories, web sites, etc.'.[330] Whether in the form of direct marketing or spam, data privacy issues arise because marketers engage in massive harvesting of an individual's

326 SALRC (n 15 above) para 512. See also B Hamann & S Papadopoulos 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) 47(1) *De Jure* 44.

327 Hamman & Papadopoulos (n 326 above) 46.

328 Hamman & Papadopoulos (n 326 above) 46.

329 Hamman & Papadopoulos (n 326 above) 46.

330 See SALRC (n 15 above) para 5.1.6 relying on S Gauthronet & E Drouard 'Unsolicited commercial communications and data protection' (January 2001) available at http://ec.europa.eu/justice/data-protection/document/studies/files/20010202_spamstudy_en.pdf (accessed 1 November 2015) 14.

personal information (both sensitive and non-sensitive) from an array of sources.[331] Most of all, such messages may be misleading or cause discomfort to data subjects.

The POPIA grants data subjects the right to object 'to the processing of personal information for purposes of direct marketing'.[332] With regard to direct marketing by means of unsolicited electronic communication, a stricter regime exists under the POPIA. Section 69 prohibits the processing of personal information for direct marketing by means of any form of electronic communication.[333] There are, however, exceptions to this provision. Direct marketing by means of unsolicited electronic communication can be carried out if the data subject has given consent or if the data subject is a customer of the responsible party.[334] With regard to the consent exception, the POPIA has unequivocally adopted an opt-in approach.[335] Products and services cannot, thus, be marketed to a data subject if he/she has not expressed his/her prior consent. This is the new approach proposed in the draft EU Regulation.[336]

With regard to the second exception for direct marketing by spam (if the data subject is a customer of the responsibility party), several conditions are placed. The responsible party can process the data subject's personal data only: if he/she (the responsible party) obtains the data subject's details 'in the context of a sale of product or service'; for marketing the responsible party's own similar products or services; and if the data subject has been given a reasonable opportunity to object. The last mentioned exception may seem like an 'opt-out' regime for direct marketing by means of unsolicited electronic communication.[337] If that is the case, the provision seems to be contrary to section 1 which provides for explicit consent otherwise known as an 'opt-in' regime. It is the view of this researcher that in case of conflicts, the provision of section 1 should prevail as it better advances the right of a data subject.

---

331 Eg customers list, telephone directory, the internet, health care providers and retail outlets.
332 POPIA, sec 5(e).
333 POPIA, sec 69. Any form of communication includes automatic calling machines, facsimile machines, SMSs, email.
334 POPIA, sec 69 (1) (a-b).
335 See SALRC (n 15 above) para 5.1.90.
336 See Recital 25 of the draft EU Regulation where it is provided that consent should be 'either by a statement or by a clear affirmative action by the data subject' and not 'silence or inactivity'. Bergkamp strongly condemns the 'opt-in' approach that '[o]pt-in, which is the functional equivalent of a property rights regime, indeed greatly enhances the autonomy of data subjects. But it does so at the expense of data controllers' autonomy. In addition… opt-in enhanced autonomy provides disincentives for creating valuable assets.' L Bergkamp 'The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy' (2002) 18(1) *Computer Law and Security Report* 33.
337 POPIA, sec 69(3)(c).

5.6.2. Automated Decision Making/ Profiling

According to the SALRC, automated decision making occurs 'where information which relates to the individual is structured in such a way that it can begin to answer questions about that person, so as to put his or her private behaviour under surveillance'.[338] This is clearly an instance where an individual loses control over the processing of his personal data, and it will be taken seriously by any contemporary data privacy law. As a general rule, automated decision making is also prohibited under the POPIA.[339] An automated decision can, however, be made if such a decision has been taken in the process of a contract and the requests of the data subject are met, or appropriate measures[340] have been taken to protect the legitimate interests of the data subject.[341] In addition, if the decision is governed by a 'law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects', then automated decision can be taken.[342]

The POPIA followed the EU Directive's provision with regard to automated decision making.[343]

5.6.3. The right to be forgotten or delete?

The right to be forgotten has been identified by Fishleigh as a contemporary issue in the 'rather edgy and menacing world of data privacy and protection'.[344] This right is basically in a bid to enhance individuals 'control over their personal data'.[345] Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship, notes that '[i]nternet users must have effective control of what they put online and be able to correct,

338 SALRC (n 15 above) para 5.2.1.

339 POPIA, sec 71. The definition of automated decision making can be deduced from the provision. Automated decision making in terms of the provision is 'a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person'.

340 The kind of appropriate measures in this regard are specified in 71 (3).

341 POPIA, sec 71(2)(a).

342 POPIA, sec 71(2)(b).

343 See art 15 of the Directive and art 20 of the draft Regulation.

344 J Fishleigh 'Is someone watching you? Data privacy and protection: Current issues' (2015) 15(1) *Legal Information Management* 61. She identified other key issues on data privacy such as right identity theft and cybercrimes. For more on the right to be forgotten, see I Szekely 'The Right to Forgotten: Personal reflections on the fate of personal data in the information society' in S Gutwirth *et al* (eds) *European data protection: In good health?* (2012) 347. See also P Bernal 'The EU, the US and right to be forgotten' in S Gutwirth *et al* (eds) *Reloading data protection law* (2014) 61-77.

345 G Zanfir 'The right to data portability in the context of the EU data protection reforms' (2012) 2(3) *International Data Privacy Law* 155.

withdraw or delete it at will.'[346] By this, Reding means that effective control especially in the online environment entails that an individual must be able to have personal information which he has uploaded on a website 'totally' removed from the cyber-space.[347] Thus, a data subject, based on the so-called right to be forgotten, can have his/her information fully removed when it is no longer needed for the purpose for which it was collected. Bernal claims that '[t]he assumption should be that unless you have a strong reason to hold it, data should not be held.'[348] The right to be forgotten is, therefore, not merely an obligation of data controllers (or responsible parties) but a right of data subjects. This right is particularly useful in the context of SNSs where an individual places certain information which may negatively affect him/her later in life.[349] With this right, a data subject could have his/her profiles totally wiped out online.[350]

The right to be forgotten is not explicitly provided for in the POPIA. Some of its effects can, nevertheless, be seen in certain conditions for lawful processing in chapter 3 of the POPIA. Section 24 generally grants a data subject the right to correction of personal information.[351] The right to correction also includes the right to 'destroy or delete a record of personal information about the data subject that the responsible party is no longer authorized to retain in terms of section 14.'[352] Similarly, section 14(5) of the POPIA provides that a responsible party must 'destroy or delete a record of personal information or de-identify it' as soon as he/she is no longer authorised to retain the record for the specific purpose for which it was collected.[353]

The POPIA's provisions given above raise questions on the relationship between the right to be deleted and the right to be forgotten. Tamò and George contend that there is a general lack of uniformity in the literature defining the whole concept of deletion of personal

346 European Commission press release database speech/10/327 speech Viviane Reding at the American Chamber of Commerce to the EU available at http://europa.eu/rapid/press-release_SPEECH-10-327_en.htm (accessed 1 November 2015).

347 SC Bennett 'The "right to be forgotten": Reconciling EU and US perspectives' (2012) 30(1) *Berkeley Journal of International Law* 162.

348 PA Bernal *Internet privacy rights: Right to protect autonomy* (2014) 200.

349 European Commission (n 336 above).

350 See I Iglezakis 'The Right to Be Forgotten in the Google Spain Case (case C-131/12): A clear victory for data protection or an obstacle for the internet?' paper presented at the 4th International conference on information law (2014). In fact based on the recent decision in the *Google's Spain case*, a search engine is responsible for contents on its site and must consider requests made by individuals for removal. This is so even if such content was contained in another website of SNS. See also Abdulrauf (n 38 above) 77-78.

351 POPIA, sec 24(1)

352 POPIA, sec 24(1)(b).

353 POPIA, sec 14(5).

information.[354] Some commentators adopt the terms 'the right of oblivion', 'the right to forget' or 'the right to delete' while others attempt to distinguish the underlying concepts based on their legal rationale and scope.[355] For example, Bernal argues that, 'the right to delete should not be seen as akin to the "right to be forgotten".'[356] Nevertheless, in another work, Bernal refers to the right to be forgotten as "one version of the idea" of a right to delete.[357] Lynskey, however, contends that the use of the phrase – 'the right to be forgotten' – is misleading.[358] Be it as it may, it is submitted that both rights have similar objectives with, perhaps, varying scope.[359]

The POPIA's provision on the right to be forgotten appears to be limited when compared to the draft EU Regulation.[360] Unlike the POPIA, the draft Regulation made the right to be forgotten an independent right granted to the data subject and an obligation on the data controller. In addition, where the data controller has made such data requested to be erased from the public, additional obligations are placed on him/her in terms of the draft Regulation. The data controller must also 'take all reasonable steps … to inform third parties who are processing such data that a data subject requests them to erase any links to, or copy or replication of that personal data.'[361] There is no equivalent of this obligation under the POPIA. The draft EU Regulation is, however, made with special reference to data made available to the data controller while the data subject was a child.[362] A number of concerns have been generally expressed with regard to the right to be forgotten. Some

---

354 A Tamò & D George 'Oblivion, erasure and forgetting in the digital age' (2014) 5 *The Journal of Intellectual Property Information Technology and Electronic Commerce Law* 72.

355 Tamò & George (n 354 above) 72,

356 Bernal (n 338 above) 201. According to Bernal, the right to be forgotten has a more negative connotation when considered with regard 'rewriting history and censorship'. Thus to describe the right to have one's information removed when it is not needed 'could…be misleading or dangerous; [as] it is not about forgetting, but about control and autonomy.' Thus '[t]alking about a right to be forgotten is attractive in some ways but it can also distract from the more important point.'

357 In this work, Bernal argues that, because of the 'extremely negative' debates the right to be forgotten has provoked, it 'needs to be renamed and recast in order to address these negative reactions and the real concerns that underlie them.' Bernal (n 261 above).

358 O Lynskey 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (2015) 78(3) *The Modern Law Review* 528

359 See Generally N Xanthoulis 'The right to oblivion in the information age: A human rights-based approach'(2013) 10 *US China Law Review* 84

360 Draft EU Regulation, art 17.

361 Draft EU Regulation, art 17(2).

362 According to Van der Sloot, '[t]he common fear that underlies this right is that children will post online pictures and videos of themselves and each other which may contain behaviour to reveal aspects of their lives which may hinder them in their development, as these videos and pictures may haunt them for the rest of their lives.' (n 155 above) 9.

of the concerns are that: it is 'a strong limitation to Internet freedom'[363] and it enables scrupulous individuals to hide useful information about their past for example, their criminal antecedence. The primary concern, however, is that advanced by Jeffrey Rosen that it affects freedom of speech and expression. The scholar contends that the right 'represents the biggest threat to free speech on the internet in the coming decade'.[364] From this perspective, an individual can prevent the circulation of important information which may be beneficial to the public. Thus, according to Bernal, the right to be forgotten has a negative connotation in that it amounts to 'rewriting history and censorship'. Perhaps this is a reason why Viviane reading observes that:

> The right to be forgotten cannot be absolute just as the right to privacy is not absolute. There are other fundamental rights which the right to be forgotten needs to be balanced be balanced – such as freedom of expression and the freedom of the press.[365]

It is submitted that the right to be forgotten should rather be understood from a narrower perspective. Generally, the right should be seen from the point of view of minimality under the processing limitation principle considered earlier.[366] From this perspective, only 'adequate' or 'relevant' information must be processed given the purpose of processing. Hence, excessive information is not adequate or relevant; as a consequence, a data subject should be entitled to have them removed. Another example is information that is no longer needed for the specified purpose under section 13 of the Act. A responsible party must 'destroy or delete' or 'de-identify' such information in terms of section 14(5). The point must also be stressed that the right can be exercised unless there are legitimate reasons provided by law to the contrary.[367] On the whole, the right to be forgotten does not grant a data subject an unfettered right to have his personal information removed. It merely states

---

363 A Mantelero 'U.S. concern about the European right to be forgotten and free speech: much ado about nothing?'(2012) *Contratto E Impresa / Europa* 727 available at http://rememberingandforgetting.wikispaces.com/file/view/US+Concern+about+the+European+Right+to+Be+Forgotten+and+Free+Speech.pdf (accessed 1 November 2015).

364 J Rosen 'The right to be forgotten' (2012) 64 *Stanford Law Review Online* 88

365 Press Release Speech Viviane Reding 'Justice for Growth makes headway at today's Justice Council' SPEECH/13/29, 18.01.2013 available at http://europa.eu/rapid/press-release_SPEECH-13-29_en.htm (accessed 1 November 2015). Indeed, art 17(3) of the draft EU Regulation provides for certain exceptions with regard to the right.

366 See 5.4.2.4 (b)

367 Zanfir (n 345 above) 155

that if the processing of such personal information is incompatible with the provisions of the POPIA, then the data subject responsible party must delete such an information.[368]

5.7. General critique of the regime of POPIA: Prospects and challenges for effective realisation of the right to data privacy in South Africa[369]

In Africa today, South Africa is a reference point on issues of information (data) privacy.[370] The POPIA was enacted at a time when debate on computerised and automated processing of personal data is growing in Africa. The POPIA contains provisions that tackle emerging challenges in the online world. It carefully blends human rights and economic objectives[371] in one document.[372] The Act, nevertheless, leaves no doubt that human rights take precedence over any other interest when it comes to data processing. The human rights' objective is further strengthened by the unequivocal link between the POPIA and the Bill of Rights in the South African Constitution. Like every modern data privacy instrument, the POPIA 'focus[es] on the individual, his interests and his right to control'.[373] This is in line with the international trend in legislating for data privacy as typified by the draft EU Regulation.[374] Thus 'increasingly detailed and specific' obligations are placed on responsible parties and more 'subjective rights' are granted to data subjects so as to enhance their control over their personal information.[375] The Act also contains a 'high level of enforcement of duties and rights.'[376] Similarly, the Act contains quite a number of innovations. Some of them are still under consideration in the draft EU

368 See Lynskey's argued with regard to the EU Directive that the right to delete only applies when the processing is incompatible with the provisions of the directive. See Lynskey (n 358 above) 528.

369 The POPIA is yet to come into force fully and, therefore, analysis in this part (especially with respect to enforcement) is only preliminary and speculative.

370 South Africa is a reference point because of the growing scholarship on human rights and privacy issues and generally, its well-considered laws.

371 The SALRC opined that '[p]rivacy is therefore an important trade issue, as information privacy concerns can create a barrier to international trade. Considering the international trends and expectations, information privacy or data legislation will ensure South Africa's future participation in the information market, if it is regarded as providing "adequate" information protection by international standards.' (n 15 above) vii.

372 Indeed, even the SALRC observed that '[t]he principles are generally held to be an acceptable compromise between the protection of personal information on the one hand and on the other hand, the use of personal information for private sector business purposes and to give effect to the responsibilities of the public sector to promote the public interest.' See SALRC (n 15 above) para 4.2.24.

373 Van der Sloot (n 155 above) 310 discussions with regard to developments in EU data privacy regime.

374 Van der Sloot (n 155 above) 310.

375 Van der Sloot (n 155 above) 310. Although some scholars are very skeptical that exercising control over what happens to one's personal data is possible. See Koops (n 191 above) 253.

376 Van der Sloot (n 155 above) 310.

Regulations. For example, the Act contains provisions relative to the protection of children's personal information which is not even contained in the EU Directive. Similarly, juristic persons are also granted rights under the Act.[377]

The POPIA has also been designed in a clear-cut manner to make it easily assessable and comprehensible to both data subjects and responsible parties. This, according to Stein, is '[a]nother area in which the drafters of POPI have benefited from the EU's experience'.[378] Thus the arrangement of the provisions is in such a way that 'the data subject's rights are easily identifiable, placing these rights at the beginning of the Bill [now Act], immediately followed by a list of the requirements for lawful processing of personal information.'[379] The FIPs are couched in a very careful and meticulous manner with specific exceptions provided for in each provision where there is an absolute need. This is unlike the approach of granting sweeping exemptions for certain individuals or some processing activities. To avoid conflicts between the POPIA and other overlapping legislation, efforts were made to ensure consistency.[380] In line with developments in the data privacy law, the POPIA contains very detailed provisions.[381] It contains 115 extensive sections.

The above notwithstanding, the POPIA, like any good law, also has some salient weaknesses. One of the shortcomings of POPIA is that certain technology-specific rights of contemporary relevance are omitted. For example, the Act does not contain the right to data portability which is surprising given the numerous threats SNSs poses to data privacy in this era.[382] The right to data portability grants individuals more control or autonomy over their personal information by enabling them to move their information from one

---

377 Granting juristic persons rights in data privacy instruments is uncommon. Eg, sec 96 of the Ghana Data Protection Act only grants natural persons right.

378 Stein (n 105 above) 48.

379 Stein (n 105 above) 48.

380 SALRC (n 15 above) para 3.1.4.

381 Van der Sloot identified the change in the trend of having more elaborate data privacy provisions right from the two Council of Europe's Resolutions of 1973 and 1974 with 8 and 10 articles respectively to the CoE Convention with 27 provisions. The EU Directive has 34 provisions and the draft EU Regulation has 91 provisions. Van der Sloot (n 152 above) 320.

382 As identified by Roos. (n 30 above). For more analysis on the right to data portability and its importance in modern day computing environment, see Zanfir (n 345 above). It is arguable that the Act does not specifically provide for the regulation of cookies in spite of its being mentioned by the SALRC as capable of collecting personal information. In this researcher's view, this goes to the broader issues of technology-specific versus technology-neutral law which will be considered in the next chapter. It is, however, important to note that data privacy laws, rarely, mention specific data privacy issues. Rather, broad principles are provided which are applicable to specific issues. The draft EU Regulation specifically mentions internet protocol (IP) addresses and cookie identifier as capable of identifying an individual, however, 'they need not be considered as personal data in all circumstances.' See Recital 24.

website (usually SNS) to another.[383] In this regard, Zanfir observes that an individual's personal information is a significant aspect of his/her personality thus, 'thinking of data collectors forbidding individuals to transfer their stack of data from one service provider to another could seem to be a violation of human rights.'[384] Similarly, the right to be forgotten is not explicitly provided for in the POPIA unlike the draft EU Regulation. Rather, elements of the right are contained in some of the conditions for lawful processing.[385] In addition, the POPIA does not contain a provision for the evaluation and review of the law.[386] A law that is technologically sensitive ought to acknowledge or make a provision for the assessment and review of the law after certain period of time because of the rapid advances in technology.

Another criticism of the POPIA is the 'one-size-fits-all' approach adopted in regulating private and public data processing in one piece of legislation.[387] Without a doubt, different sectors present unique challenges to the data privacy right. While the majority will argue that the private sector presents a greater challenge to data privacy, others will see the public sector as more threatening.[388] Trying to regulate all data privacy issues in one document can, therefore, be said to be too ambitious.[389] Even Neethling *et al* appear to appreciate this point when they posit that:

> Due to the multifaceted nature of the data industry, it would at first glance appear to be impossible to adopt only a single generally valid statutory measure regarding the protection of data. A differentiated approach therefore seems to be necessary, depending on the nature of the entity compiling information, the type of personal data collected and the purpose for which it is to be used.[390]

---

383 Swire & Lagos have, however, criticised this right as provided under the draft EU Regulation that it is not well-defined and established and no jurisdiction has experimented with anything like it before. See P Swire & Y Lagos 'Why the right to data portability likely reduces consumer welfare: Antitrust and privacy critiques' (2013) 72 *Maryland Law Review* 380.

384 Zanfir (n 345 above)151

385 As discussed in 5.6.3 above.

386 See, eg, art 90 of the draft EU Regulation which provides that: 'The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.'

387 See discussions in Koops (n 191 above) 259-259.

388 Bergkamp (n 336 above) 36.

389 As even the EU have certain instruments on data privacy with sector-specific application.

390 Neethling (n 1 above) 272.

The authors were, nonetheless, quick to state that having different regimes for data privacy protection may be too cumbersome, complex and rigid.[391] On a similar note, Kuner sounds a note of caution on the increasing blurring of the line between data being processed in the public and private sectors as law enforcement agencies often seek access to personal data being processed in the private sector.[392] Kuner's warning appears to affirm the fact that modern day data processing activities makes it difficult to distinguish among data being processed in the various sectors. Similarly, in an analysis of the proposed reforms in the EU regime on data privacy,[393] it was observed that the distinction between personal data on a sectoral basis is more 'schematic and artificial'.[394] This is because of the relative ease and systemic access of public data processors to private sector data and *vice versa*. On this basis, it is our view that the POPIA's approach has some merits.

The EU Directive and draft EU Regulation have been criticised for certain manifest inconsistencies in the FIPs[395] which also seem to be replicated in the POPIA. The EU Directive, for example, provides for conditions for lawful processing in articles 6 and 7.[396] Article 6 of the Directive (now article 5 of the draft Regulation) contains 'principles relating to data quality' while article 7 (now article 5 of the draft Regulation) provides for 'criteria for making data processing legitimate'. It has, therefore, been argued that '[n]o clear guidance was given in the text of the Directive regarding the relationship between them' which may lead data controllers to 'adopt…an opportunistic approach, whereby they choose either to apply [any of the provisions] to justify the legitimacy of their processing'.[397] A similar situation also seems to be present in POPIA. Sections 8-25 provide for 'conditions for lawful processing of personal information' while section 11 particularly stipulates requirements for processing of personal information. Unlike the EU Directive (and draft Regulation), however, section 11 is subsumed under chapter three as part of the general conditions for lawful processing. Thus a responsible party does not have the liberty to choose which to apply under the POPIA. It is, therefore, submitted that the POPIA's approach is consistent and preferable.

391 Neethling (n 1 above) 272.
392 C Kuner *Transborder data flows and data privacy law* (2013) 18.
393 Especially with respect to sectoral application of certain data privacy instruments.
394 De Hert & Papakonstantinou (n 104 above)132.
395 De Hert & Papakonstantinou (n 104 above)135.
396 Draft EU Regulation, arts 5 & 6.
397 De Hert & Papakonstantinou (n 104 above)135.

On the whole, Roos posits that the Act[398] 'complies, in all important aspects with international standards.'[399] On his part, Van der Merwe is hopeful that the 'law will finally make concrete the lofty ideals with regard to privacy expressed in the Constitution.'[400] It is, hence, submitted that the Act presents useful lessons for Nigeria.

5.8. South Africa and international/regional data privacy regimes: Extent of influences?

All data privacy legislation in countries with one have been substantially influenced by international or regional data privacy frameworks.[401] South Africa is not an exception to this. The POPIA has obtained substantial guidance from major international data privacy regimes even though South Africa is not a signatory to any of these instruments.[402] As mentioned earlier, however, the influence of the EU's regime is preeminent.[403] This fact is vindicated by the final report of SALRC where countless references were made to the EU Directive as a benchmark in deliberation.[404] This is not surprising as EU Directive has 'now become the international data protection metric against which data protection adequacy is measured.'[405]

To justify its affiliations with international data privacy regimes further, the preamble of the POPIA unequivocally states that the parliament of South Africa enacts the legislation (POPIA) in order to regulate the processing of personal information 'in harmony with

398 Her discussion was when the Act was still in the drafting processes.
399 Roos (n 10 above) 389.
400 D Van der Merve 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17(1) *Potchefstroom Electronic Law Journal* 305.
401 See generally G Greenleaf '76 Global data privacy laws' (September 2011) 112 *Privacy Law and Business Special Report* 3. See also SALRC (n 15 above) para 4.1.8.
402 The Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data and the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention). See SALRC (n 15 above) para 4.1.8. Unlike the CoE Convention on cybercrime wherein South Africa is a non-member signatory, it is not a signatory of the CoE Convention on data privacy.
403 See Roos (n 30 above) 379 referring to the Bill which subsequently became the POPIA. Both the EU Directive and the draft EU Regulation.
404 Several references are made to the EU Directive as the benchmark in determining what and what should be considered in the debate and discussion. In fact, reference was not only made to the Directive but the draft EU Regulation. See AB Makulilo ' "One size fits all": Does Europe impose its data protection regime on Africa' (2013) 7 *Datenschutz und Datensicherheit* 450
405 De Hert & Papakonstantinou (n 104 above)131.

international standards'.[406] The SALRC gave a possible rationale for its interest in making the POPIA to be in harmony with international standards. It was pointed out that '[s]pecific reference to international standards will imply that relevant international instruments and jurisprudence may be consulted in order to assist when interpreting and applying the legislation.'[407]

Because data privacy law is still in an infant stage in Africa, regional and sub-regional instruments have had little or no influence on data privacy regimes in Africa.[408] For example, South Africa belongs to the African Union (AU) and the Southern Africa Development Community (SADC) at the regional and sub-regional levels. Although both organisations have data privacy instruments which were in existence before the passing of the POPIA,[409] no reference was made to them in the preparatory works leading up to the POPIA.[410] These African instruments did not influence developments in South Africa, because the SALRC, arguably feels it is better to draw lessons from the more mature EU regime rather that a relatively new African instruments.

Be that as it may, even after enacting the POPIA, certain provisions show that its regime is still open to international (external) influences so as to boost data privacy protection.[411] This ensures that the law and legal regime does not operate in isolation. In terms of the POPIA, the Information Regulator is to conduct research and report to parliament on the desirability of the acceptance of any international data privacy instrument.[412] The Information Regulator is also to facilitate transborder cooperation in the enforcement of privacy laws by participating in initiatives in that regard.[413] Even the AU Data Protection

---

406 See the preamble to the POPIA. Indeed Roos observes that international data protection instruments have an added purpose, namely to harmonise data protection laws in signatory countries. Roos (n 10 above) 317.

407 SALRC (n 15 above) para 3.2.7.

408 Bygrave (n 129 above) 80. Makulilo (n 404 above) 450.

409 The SADC has a SADC Data Protection Model Law (2012) with objective, among others, of harmonizing data privacy polies and laws among member states. For more discussions on the Model law, see Makulilo (n 5 above) 85.

410 See Makulilo (n 404 above) 450. The present AU Convention on Data Protection came into force in 2014. Nevertheless, there was the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa of 2011 and the African Union Convention on the Confidence and Security in Cyberspace of 2013 with both data privacy provision, though it arguable in another vein that the discussion preparatory to the POPIA commenced quite a bit earlier.

411 South Africa has always tried to ensure that its law is in line with international law. Sec 233 of the South African Constitution provides that 'when interpreting any legislation, every court must prefer any reasonable interpretation of the legislation that is consistent with *international law over any alternative interpretation that is inconsistent with international law*'. (Emphasis added).

412 POPIA, sec 40 (1)(e)(i).

413 POPIA, sec 40(1)(g).

Convention encourages member states to cooperate with third countries.[414] Thus, National Data Protection Authorities must establish 'mechanisms for cooperation with the personal data protection authorities of third countries' and must also 'participate in international negotiations on personal data protection.'[415] Provisions on international cooperation will obviously enrich South Africa's regime on data privacy. This is indeed a vital insight for Nigeria.

5.9. Chapter conclusion: Lessons from an 'African' data privacy regime

This chapter has analysed the extant legal framework for the protection of data privacy in South Africa with a view to drawing lessons for Nigeria. The discussion in this chapter is particularly useful because the South African regime is a reflection of the international data privacy standard in an African setting. This is important for data privacy challenges peculiar to African countries which, as we have argued, are quite similar in certain respects. Based on the similarities of data privacy challenges faced by Nigeria and South Africa, the question is whether there are useful insights to be gained from South Africa in realising adequate protection of data privacy.

In answering this question, an analysis was carried out on the conceptual basis and approach to data privacy protection in South Africa. Here, it was argued that South Africa has largely adopted the EU's approach in data privacy protection. This approach involves constitutional provisions, on the one hand, supported by comprehensive legislation which regulates data processing activities of both private and public entities on the other. The conceptual basis of data privacy protection in South Africa was also argued to be for the protection of dignity which is in line with what obtains in the EU. Nevertheless, it was also submitted that *Ubuntu*, which is an African philosophy, also has its influence in data privacy protection in South Africa. This is because *Ubuntu* is all about human dignity and dignity is a core value in the South African Constitution. In this respect, the conceptual basis of data privacy is similar to that in the EU.

Based on the international trend, this chapter has focused on the constitutional and statutory protection of data privacy in South Africa. The statutory regime in this regard is a specifically dedicated piece of legislation on data privacy. An analysis was carried out on

414 See art 12 (2).
415 Art 12 (2).

the South African Constitutional provision on data privacy and the POPIA. It was observed that, although data privacy is not explicitly contained in the South African Constitution, the Constitutional Court has given the right to privacy an expanded interpretation to cover data privacy (information privacy). Thus a contemporary problem which was not anticipated when the Constitution was being drafted is recognised by the progressive interpretation of the Constitution by the court. This is indeed a vital insight for Nigeria.

An elaborate discussion was also carried out on the substantive aspects of the POPIA that are important for the realisation of adequate protection of data privacy. In this discussion, the study found that the POPIA is another progressive instrument with a number of useful innovations for the realisation of the rights of data subjects. Firstly, in line with contemporary practice on legislating for data privacy, more rights are granted to individuals so as to enhance control over their personal data. Secondly, the POPIA contains internet-specific rights which are an acknowledgement of the contemporary and future challenges to data privacy. Despite the ambitious provisions of the POPIA, certain weaknesses were identified with the provisions of the Act which may require reconsideration. One such weakness is the omission of certain internet-specific rights like the right to data portability and the lack of provision on review of the Act.

It is very important that the data privacy regime operates in concert with other international and regional frameworks on data privacy. In this regard, an analysis was carried out of the influence of the international and regional data privacy framework on the South African data privacy regime. Also, provisions on international cooperation in the POPIA were examined.

Although the POPIA is a new instrument that is yet to be fully operational, there is already evidence that there will be wide compliance with its provisions. For example, the University of South Africa (UNISA) recently stated that it is in compliance with the Act and efforts are being made to ensure that its affiliated institutions also comply.[416] Similarly, Momentum Health has also shown that the use of members' personal

[416] University of South Africa (UNISA) 'Compliance with the Protection of Personal Information (POPI) Act' http://www.unisa.ac.za/news/index.php/2015/03/compliance-with-the-protection-of-personal-information-popi-act/ (accessed 1 November 2015).

information is only in accordance with the POPIA.[417] All in all, it submitted that useful lessons can be obtained from the South African experience for the purpose of realising the right to data privacy in Nigeria. The next chapter, therefore, discusses the 'rights-based' approach to data privacy based on a comparative analysis of selected focus areas in the Canadian and South African regimes.

417 Momentum Health 'International student application form' http://www.ingwehealth.co.za/Files/(20141110113238%20AM)%20STUDENTHEALTH005_0115E_International_Student_Application_form_fillable.pdf (accessed 1 November 2015).

Chapter six

Prospects for improving data privacy regimes: A proposal for a 'rights-based' approach (in Nigeria)

6.1. Introduction

> *If human rights that are considered important are to be protected, fostered and supported, then privacy and autonomy need to become the default. Surveillance and breaches in privacy need to be the exception, and exist only when truly justified.*[1]
>
> *Human rights first, then market after.*[2]

Chapters four and five of this thesis considered the protection of the *sui generis* right to data privacy in Canada and South Africa where quite a number of useful insights were gathered. This study does not stop there. The thesis goes further now to take a closer look at how a data privacy regime can be designed towards better utilisation in realising the data privacy right in the light of contemporary debates. Because of the peculiar situation of Nigeria[3] a rights-based approach is proposed. A rights-based approach, though not a new idea in data privacy law, is particularly suitable because of misconceived objectives of

---

1 P Bernal *Internet privacy rights: Rights to protect autonomy* (2014) 288. See also PA Bernal 'Do deficiencies in data privacy threaten our autonomy and if so, can informational privacy rights meet this threat? Published PhD thesis, London School of Economics and Political Science, 2013 317.

2 AJ Cerda Silva 'Internet freedom is not enough: Towards an internet based on human rights' (2013) 18 *SUR International Journal of Human Rights* 27. He further stressed that '[a] human rights-based internet must give preference to human rights rather than market.' Although his discussion is restricted to human rights issues on the internet, it is relevant to my approach in advancing a rights-based approach thesis.

3 The peculiar situation of the country has been elaborately discussed in chapter 3. In summary, Nigeria is characterised by relative advances in technological development without a corresponding legal regime to tackle challenges that results from such advances.

legislating for data privacy in Africa (and Nigeria).[4] It was argued in chapter two that data privacy regimes are basically for the purpose of realising two main objectives - protecting data privacy rights of individuals and promoting the free flow of personal information for economic (market) purposes. It was also pointed out that, in many instances, the first mentioned objective is usually sacrificed on the altar of the second.[5] This is, indeed, an unhappy state of affairs for human rights and fundamental freedoms. For the sustenance of individuals' rights to autonomy and dignity, it is, therefore, important that human rights are at the centre of the current data revolution.[6] Data privacy protection in African countries must give utmost consideration to human rights.

This chapter, therefore, advances the rights-based thesis as conceived by some legal scholars while comparing the Canadian and South African regimes (and beyond). Analysis in the chapter is carried out based on selected focus areas in the regimes of the countries

---

4 Some authors have argued that enacting data privacy laws in Africa is mainly for economic purposes (to satisfy the EU Directive's adequacy requirement) without due consideration of actual protection of data privacy. Makulilo, however, seems not to agree with this theory as far as explaining the rationale for data privacy protection in Africa. According to this scholar 'there is currently no general survey to concretise the extent to which African countries have economically been affected by the restriction on transfer of personal data from Europe. In most cases such claims have been made by sweeping statements.' AB Makulilo 'Protection of personal data in sub-Saharan Africa' published Dr. Jur. thesis, University of Bremen, 2012 266. The thesis was published as AB Makulilo *Privacy and data protection in Africa* (2014). Various attempts to get a copy of the book proved abortive.
I disagree with the scholar's view above on the purpose for enacting data privacy laws in some African countries on several grounds. One such ground is the fact that most African countries, with the exception of South Africa, do not engage in sufficient debate before passing such laws. Nigeria is a case in point where there are no publicly available documents on the debates on any of the Data Protection Bills. Rather, all the draft bills are merely 'cut and paste' of international data privacy laws. Moreover, most scholarship on data privacy in Nigeria seem to be arguing for enacting data privacy laws so as to be able to benefit from outsourcing or trade with the EU. See for example A Kusamotu 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European Union Directive 95/46' (2007) 16(2) *Information & Communication Technology Law* 149-159. See also AKE Allotey 'Data protection and transborder data flows: Implications for Nigeria's integration into the global network economy' unpublished LLD thesis, University of South Africa, 2014.
Makulilo's views seem to have changed in more recent works where he recommended that 'African governments should not only adopt data privacy legislation for the purposes of attracting foreign investments but also to help their people against unauthorised processing of personal data.' AB Makulilo 'Data protection regimes in Africa: Too far from the European 'adequacy' standard?' (2013) 3(1) *International Data Privacy Law* 50.

5 Perhaps this is a reason why Greenleaf recently notes that '[i]t is often said that [data] privacy is impossible to protect, either against governments or corporations. States develop comprehensive information systems concerning their citizens. Local businesses want to 'know their customers', and international businesses that run global social networks, search engines and the like, gather unprecedented amounts of personal information on their users.' G Greenleaf *Asian data privacy laws: Trade and human rights perspectives* (2014) 3.

6 IMC Barroso & K Goulven 'A rights-based revolution' http://www.undatarevolution.org/2014/10/14/rights-based-revolution/ (accessed 1 November 2015).

considered.[7] In addition, the chapter engages contemporary legal scholarship on the trend of debate towards improving data privacy protection from a rights-based perspective.

In the light of these debates, part 6.2 of the chapter expands on the conception of a rights-based approach as discussed in chapter two and examines its value to African countries. Possible arguments against the rights-based approach will also be discussed in this part. Part 6.3 examines the role of the constitution (Bill of Rights) in a rights-based approach to data privacy. The next part (6.4), discusses statutory protection of data privacy and the rights-based approach. Here I focus on how preliminary provisions in a data privacy instrument can be tailored towards promoting the interests and rights of a data subject. Part 6.5 which considers the fair information principles (FIPs) and the rights-based approach ought to be discussed as part of the previous section. Because of the crucial role of the FIPs to a data privacy instrument and the rights of individuals, it will, however, be discussed separately.[8] Part 6.6 reflects on the role of data protection authorities (DPAs) in advancing a rights-based approach to data privacy protection. Furthermore, part 6.7 considers the debates regarding how 'new technologies' can be used to promote data subjects' rights to have control over their personal information. Part 6.8 briefly applies the rights-based approach to some data privacy challenges in Nigeria as identified in chapter three.

6.2. An analysis of a rights-based approach to data privacy protection

A rights-based approach is by no means a new idea in the field of human rights law although it is seldom used with regard to data privacy.[9] Nevertheless, it is submitted that

---

7 Copious references are also made to the EU regime especially the draft EU Regulation because it is introducing novel policies aimed at promoting a truly 'rights-based' data privacy regime in line with the central thesis of this chapter.

8 To further justify the value of these principles, some legal scholars see the principles as the substance of data privacy law. Eg, Greenleaf defines data privacy as "a set of 'data protection principles', which include an internationally accepted set of minimum principles plus additional principles which are evolving continually through national laws and international agreements." Greenleaf (n 5 above) 5.

9 However, discussions on a rights-based approach are usually associated with socio-economic rights in general and the right to development in particular. For more on such conception of a rights-based approach, see P Uvin 'From the right to development to the rights-based approach: How 'human rights' entered development' (2007) 17(4-5) *Development in Practice* 597-606; C Nyamu-Musembi & A Cornwall 'What is the "rights-based approach" all about? Perspectives from international development agencies' working paper series, 234 Brighton: IDS available at http://opendocs.ids.ac.uk/opendocs/handle/123456789/4073#.Vc2TC7Vu6Wg (accessed 1 November 2015). See D Olowu *An integrative rights-based approach to human development in Africa* (2009).

the idea of a rights-based approach has always been connected with data privacy from the beginning of debates on the need for the protection of personal information.[10]

6.2.1. An explanation of a rights-based approach

This thesis has, from the outset, put forward the claim that a rights-based approach is more likely to be effective in realising adequate protection of data privacy in a country than any other approach.[11] For the purpose of emphasis, a rights-based approach can be explained from two perspectives based on Paul Bernal's postulation.[12] The first way to determine whether a data privacy regime is rights-based is the normative basis of such a regime. Secondly, is the interest which such a regime seeks to foster or promote. With regard to the normative basis (core ethical value) of a data privacy regime, Bernal is of the view that, if an instrument has its origin and legal basis in the right to privacy (in a human rights instrument or Bill of Rights), it is in principle 'right-based'.[13] Most data privacy instruments are normatively based on the right to privacy.[14] That is why the European Union's (EU) regime (especially, the EU Directive) is generally considered to be rights-based.[15] This explanation of a right-based approach may, however, be problematic because not every data privacy law that is considered 'right-based' is founded on the right to privacy. In some cases, data privacy instruments are normatively based on some other human right. For example, the German data privacy law is founded on the right to informational self-determination which is an independent fundamental right based on the rights to dignity and personality.[16] Similarly, the draft EU Regulation is based on the

---

10 From the outset, data privacy protection has always been linked to the human right to privacy. Thus the first set of rules, especially in Europe, based data privacy on human rights. The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981) (CoE Convention) was based on the human right to privacy. For more analysis on these issues, see M Albers 'Realizing the complexity of data protection' in S Gutwirth *et al* (eds) *Reloading data protection: Multidisciplinary insights and contemporary challenges* (2014) 214-215.

11 Chapter 1 (1.1) above.

12 Bernal is one the very few authors who used the term 'rights-based approach' with respect data privacy protection. His discussion was, however, restricted to privacy rights on the internet. See generally Bernal (n 1 above).

13 He pointed out that '[i]n principle it [the EU Directive] is 'rights-based', at least in the sense that its origins include Article 8 of the European Convention on Human Rights, the right to respect for privacy (embracing a right to a private life).' Bernal 2014 (n 1 above) 223.

14 See discussions in chapter 2 above. Examples are CoE Convention, Art 1; EU Directive, Art 1 and Protection of Personal Information Act (POPIA) Act 4 of 2013, sec 2.

15 Many scholars generally refer to the EU regime as rights based. See eg, JM Victor 'The EU General Data Protection Regulation: Toward a property regime for protecting data privacy' (2013) 123 *The Yale Law Journal* 515.

16 See the German *Population census decision* Judgment of 15 December 1983 Bundesverfassungsgericht, decisions vol 65. The German Federal Constitutional Court (Bundesverfassungsgericht) established the right to informational self-determination based on German Basic Law (Deutscher Bundestag, Basic

newly-established right to data protection.[17] It is the view of this researcher that, in principle, if a data privacy instrument has its normative basis in any human right, it is rights-based.[18] Kosta seems to capture this view more effectively when she contends that a rights-based approach 'in simple terms bases data protection on fundamental rights of the data subject.'[19]

In practice, however, Bernal contends that a data privacy regime is rights-based if it is genuinely 'individual-centred'.[20] This researcher has earlier argued[21] that regulation (legislating) for data privacy is mainly for two broad reasons. The first is for the data privacy rights of individuals, and the second is for the purpose of promoting the free flow of personal information.[22] It is contended that a regime or a legal instrument that accords greater value to the former is rights-based.[23] Seen in this light, a data privacy regime should concentrate on 'the individual, his [or her] interests and his [or her] right to control'[24] the processing of his/her personal data.[25] Data privacy should be treated more as

---

Law for the Federal Republic of Germany https://www.btg-bestellservice.de/pdf/80201000.pdf); arts 1(1) and 2(1). The provisions provide for the rights to human dignity and personality respectively. For more in-depth analysis of the decision, see G Hornung & C Schnabel 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25(1) *Computer Law & Security Report* 84-88. Similarly, although the French Data Protection Act provides in art 1 that information technology 'shall not violate human identity, human dignity, privacy, or individual or public liberty', more emphasis is placed on liberties. See Commission nationale de l'informatique et des libertés (CNIL) Loi Informatique et Libertes Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties. Available at http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (accessed 1 November 2015). For more detailed analysis, see GG Fuster *The emergence of personal data protection as a fundamental right of the EU* (2014)174.

17 Proposal for a Regulation of the European Parliament and 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 or draft EU Regulation), art 1(2). See also Charter of Fundamental Rights of the European Union (2000/C/ 364/01) (EU Charter), art 8.

18 It must be pointed out that, in the US, data privacy seems to be built on other values with are not human rights. De Hert and Gutwirth contend that data privacy is built on public law principles such as fair information practices in the US. See P De Hert & S Gutwirth 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in Act' in S Gutwirth *et al* (eds) *Reinventing data protection?*(2009) 10.

19 E Kosta *Consent in European data protection law* (2013) 138.

20 Although his comments in this regard were particularly directed at the EU Directive or the EU regime on data privacy generally.

21 In chapter 2 (2.5).

22 Promoting the free flow of information serves economic purposes as argued in chapter 2. Economic purposes in this regard also include for protectionist benefits. Indeed, Bygrave argued the EU Directive may serve protectionist value for data controllers in the EU. LA Bygrave *Data protection law: Approaching its rationale, logic and limits* (2002) 115.

23 Bernal 2014 (n 1 above) 223.

24 Indeed many theorists have defined privacy in terms of control. See A Westin *Privacy and freedom* (1967) 7. For an update version of his views, see A Westin *Privacy and freedom* (2015).

25 B Van der Sloot 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 310.

a human right rather than a mere interest which should compete with other less significant interests (like, enhancing market). From this perspective, Lindsay and Ricketson distinguish a *rights-based approach* from an *interest-based approach*.[26] In their view, the EU Directive is an example of a 'rights-based approach' while the Australian Privacy Act is an example of an 'interest-based approach'.[27] Yet, Bernal criticises the EU regime (especially the EU Directive) arguing that '[t]hough the data protection regime has some of its roots in rights, its realities are more focussed on economic drives – rights are treated more as a qualifier, an influence, but not as the backbone of the regime.' [28]

The second conception of a rights-based approach advances the notion of informational self-determination which is, arguably, the essence of data privacy law.[29] Thus, a data privacy regime should strictly focus on the underlying right to autonomy and dignity of a

---

26 D Lindsay & S Ricketson 'Copyright, privacy and digital rights management (DRM)' in AT Kenyon & M Richardson (eds) *New dimensions in privacy law: International and comparative* perspectives (2006) 141.

27 The scholars were further of the view that a rights-based approach can be distinguished from an interest based approach based on the scope of data protection law and the nature of rules and principles contained in the law. They argued that "[l]aws that adopt a 'rights-based' approach to data protection appear to have a broader scope than laws with an 'interest-based' perspective'. Similarly, both approaches can be distinguished based on the nature of exemptions and exception found in the law and other contents of the law like consent requirement. see Lindsay & Ricketson (n 26 above) 140-142

28 Bernal 2014 (n 1 above) 223. He further contends, with regard to the draft EU Regulation, that 'it appears unlikely, however, that fundamental changes will be suggested, and so it remains probable that the focus of data protection will remain, as its name suggests, on the data, rather than on the individual'. Van der Sloot, on the other hand, has a different opinion. She is of the view that the proposed review is towards making the regime more rights-based as there are more rights bestowed on the individuals with regard the processing of his personal data. See generally Van der Sloot (n 25 above). Lynskey also thinks that the rights-based objectives of the draft EU Regulation are promoted when she contends that 'new rights are introduced, old rights are reinforced and more effective enforcement mechanisms are set out.' O Lynskey 'From marketing-making tool to fundamental right: The role of the Court of Justice in data protection's identity crisis' in S Gutwirth *et al* (eds) *European data protection: Coming of age* (2013) 81. Similarly, De Hert and Papakonstantinou are of the view that the draft EU Regulation 'marks the second generation of data protection regulatory instruments at the EU level…and a definite cause for celebration for human rights.' P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 142.
On the other hand, the view was expressed with regard to the OECD Guidelines and the APEC Privacy Principles that '[i]n all of these instruments, the free flow of information is used to clarify the degree of protection that will be provided to the right to privacy and personal data protection'- thus, placing so much emphasis on the market objectives rather than human rights.' Creda Silva (n 2 above) 23.

29 Especially based on the European conception. See the *German population census case* (n 16 above). Lindsay and Ricketson noted that '[t]he approach adopted in the Census decision is an essential part of the conceptual background to the 1999 European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free movement of Such Data, which established new benchmarks for the protection of personal data of European Union citizens.' Lindsay & Ricketson (n 26 above) 136. See also Albers (n 10 above) 214-215.

data subject.[30] In pushing Bernal's argument further, it is submitted that a data privacy regime that is rights-based should further empower individuals to exercise greater control over their personal information. The scholar explains that:

> [a] more direct and genuinely rights-based approach would put that focus (privacy and autonomy) back on the rights of the individual. It would look at issues from the perspective of the individual, and how the individual experiences things, how the individual is affected by events, and how the individual can understand those events, rather than the precise and technical details of what may or may not be happening to particular pieces of data.[31]

The difficulty of realising effective data privacy in practice inspires the need for a paradigm shift. Thus, the rights-based approach is all about *strengthening* and *refocusing* the core object of data privacy protection which seems to be overlooked because of the overshadowing or competing interests in the processing of individuals' personal information.[32] Indeed, De Hert and Gutwirth point out that data privacy is a series of ideas used by the government 'to reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc.'[33] Schartum also observes that '[d]ata protection and privacy are under pressure from actors who advocate other political objectives that enjoy considerable support and legitimacy in the population at large."[34] Because of the competition data privacy rights receive at various ends, it is important that more effective initiatives are put in place so that individuals do not lose their sacred power of control, in this case strict data privacy measures.

Since the realisation of adequate data protection is proving so difficult in practice, a rights-based approach as conceived in this chapter is apt. The rights-based approach brings together various regulatory strategies/mechanisms based on the constitution, legislation, enforcement and oversight institutions and the use of other regulatory mechanisms (new

30 See L Stefanick *Controlling knowledge: freedom of information and privacy protection in a networked world* (2011) 59.

31 Bernal (n 1 above) 223.

32 I have discussed the benefits derived from the processing of personal data to both private and public entities in chapter 2(2.2) of this thesis.

33 De Hert & Gutwirth (n 18 above) 3.

34 DW Schartum 'Designing and formulating data protection laws' (2010) 18(1) *International Journal of Law and Information Technology* 1. The author further noted that 'data protection may be seen as something *secondary* in relation to the process of using ICT to reconstruct the machinery of government, revitalize the political system, renew commerce, and other fundamental and powerful societal and political changes.' 4.

technologies). It also proposes the harmonious working of the entities subject of data privacy law which are the data controllers (responsible parties),[35] data subjects and DPAs.

6.2.2. The need for a rights-based approach to data privacy protection in African countries

A discussion on a rights-based approach is particularly significant for African countries. This is because of the view put forward by some scholars that African states, arguably, do not have much regard and value for (data) privacy.[36] Rather, they merely enact data privacy laws to satisfy the EU's adequacy requirement.[37] In short, data privacy regimes in Africa are arguably there for economic purposes – largely to enhance trade opportunities with the large EU bloc. As Nova puts it, '…the prospect of a gigantic twenty five member trading block adhering to these provisions [the EU Directive] makes the Data Directive almost impossible to ignore.'[38] Bygrave, therefore, contends that one of the reasons for the emergence and development of data privacy laws in Africa is that of 'economic concerns, particularly the desire by some of these countries to safeguard their outsourcing industry.'[39] Similarly, Makulilo points out that:

> It is noteworthy that a powerful driver of the development of [data] privacy law among developing countries is the desire to engage in global e-commerce and the recognition of trust as being a fundamental component of the new economy. Undoubtedly this has been the paramount motivation for the adoption of data privacy legislation in Africa. Invariably almost, protection of [data] privacy as such appears only a secondary agenda. This is perhaps due to the little public concern for [data] privacy.[40]

---

35 For the purpose of this chapter, data controllers, data processors and responsible parties will be used interchangeably. Where discussions are, however, specifically based on a particular jurisdiction, the term adopted by that jurisdiction will be used.

36 For a more elaborate consideration of these debates, see AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) *International Data Privacy Law* 171.

37 See discussions in (n 4 above). See also AB Makulilo " 'Peel off the mask': Enforcement of Data Protection Act in Mauritius'(2014) 12 *Datenschutz und Datensicherheit* 847 where the learned scholar argued with regard to the Mauritius Data Protection Act, that it was adopted to secure economic investments.

38 TD Nova 'The future face of the worldwide data privacy push as a factor affecting Wisconsin businesses dealing with consumer data' (2004) 22(3) *Wisconsin International Law Journal* 792.

39 LA Bygrave 'Privacy and data protection in an international perspective' (2010) *Stockholm Institute for Scandinavian Law* 194.

40 AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 79. In yet another work, the scholar argues that 'those few African jurisdictions which have so far adopted data protection legislation have largely done so for economic motivations…' See AB Makulilo '"One size fits all": Does Europe impose its data protection regime on Africa?'(2013) 7 *Datenschutz und Datensicherheit* 450.

A practical manifestation of the above scholar's observation can be seen in a comment by the South African Law Reforms Commission (SALRC) in the discussions preparatory to the Protection of Personal Information Act (POPIA) where the view was unequivocally expressed that the 'POPIA has been drafted with the object of providing South Africa with an EU adequacy rating to ensure free TBDF'.[41] All these show that there is an urgent need for a re-orientation on the basis and importance of data privacy protection in Africa in general and Nigeria in particular. Stronger and more focused regimes which should redirect the data privacy objective to the protection of individuals are, therefore, imperative.

6.2.3. Arguments against a rights-based approach to data privacy protection

Quite a number of arguments have been made by scholars against an 'individual-centred' data privacy regime which has a connection with the rights-based thesis conceived in this chapter. The majority of these criticisms are, however, on the basis that it affects market and trade.[42] Since this argument has been briefly considered in chapter two (2.9), it will not be repeated here. The focus of this part is on arguments against the philosophy of granting individuals more power of control over their personal information, that is, informational self-determination. In other words, on what basis should data privacy law give utmost priority to the interests and rights of individuals? Van der Sloot captures the crux of these issues in a succinct manner.[43] In her view, the main problem with this approach is that there are uncertainties with regard to the basis for individuals to have control over non-private and non-sensitive data, group profiles, and statistical correlations.[44] This is so because '[t]he definition of personal data has been increasingly disconnected from the physical person'.[45] With regard to private and sensitive information, a justification exists for an individual to exercise control since its processing interferes with his/her private life. But according to Van der Sloot, such is not the case for public and non-sensitive data.

---

41 See South African Law Reform Commission (SALRC) 'Privacy and data protection report' (2009) para 5.3.40 available at www.justice.gov.za/salrc/dpapers/dp109.pdf (accessed 1 November 2015).

42 L Bergkamp 'The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy' (2002) 18(1) *Computer law & Security Report* 31-47.

43 The arguments considered here are not stated by the author as 'criticisms of a rights-based data privacy regime'. Issues raised here are based on the draft EU Regulation where increasing emphasis is placed on the rights of individuals. This is relevant because the ideas behind the reforms (draft EU Regulation) inspire my thesis of a rights-based approach.

44 Van der Sloot (n 25 above) 322.

45 Van der Sloot (n 25 above) 322.

It is submitted that, taken from the perspective of scholars and jurisdictions who see personal information (as narrowly construed) as part of private information, a clear justification exists for its protection. In other words, both Canada and South Africa, for example, see personal information (in its public and non-sensitive form) as part of private information. Based on this perception, there are, therefore, sufficient justiciable grounds to grant the individual more and more rights to control its processing. Difficulties, however, arise where personal information is perceived as largely removed from the realms of private information (which this thesis suggests).[46] In other words, why should personal information, which is neither private nor sensitive, be afforded greater protection? In a seeming response to this question, Birnhack points out that:

> …the problem is that someone else decides who we are, ripping us of self-control. Thus understood, the control of personal data is a matter of human dignity. A person should be treated as a moral, independent agent, capable of deciding his or her own path in life. The seamless collection of data, its accumulation and subsequent processing slowly transfers our personhood to control of others, usually corporations.[47]

Based on Birnhack's comments above, there is sufficient ground for a genuine rights-based approach to data privacy especially in this era of advances in technology. Moreover, there is an emergent school of thought that seems to be advocating greater power of control for individuals on the basis of property rights. Purtova, for example, argues that there are sufficient grounds for granting an individual power of control on the basis of property right and the increasing commodification of personal information.[48] An individual's personal information is, therefore, his/her property and he/she must exercise the attendant rights that come with ownership. Another criticism of the approach is its feasibility[49] which, in this researcher's view, is not a structural weakness. Since the risks of data processing are clearly established, better ways to ensure the realisation of data privacy should be sought,

---

46 Hence the *sui generis* right. The research views in this regard are largely based on arguments by O Lynskey "Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order" (2014) 63(3) *International and Comparative Law Quarterly* 569-597.

47 MD Birnhack 'The EU Data Protection Directive: An engine of a global regime' (2008) 24(6) *Computer Law & Security Report* 509.

48 N Purtova *Property rights in personal data: A European perspective* (2012). Rouvroy & Poullet, however, rejected the idea of property rights in personal data. They argued that medical data, eg, arguably belongs to the medical practitioner in charge of the patient as well as the patient himself/herself. A Rouvroy & T Poullet 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy' in S Gutwirth *et al* (n 18 above) 72.

49 Van der Sloot (n 25 above) 322. See also B Koop 'The trouble with European data protection law' (2014) 4(4) *International Data Privacy Law* 250-261.

rather than finding excuses. This researcher has examined the immense benefits of personal data to data controllers and even an individual data subject[50] which creates varying interests in data processing. The point must, however, be made that, in fostering these interests, human rights of individuals must be prioritised. Birnhack contends that the argument that data privacy regimes conflict with the interests (commercial and other purposes) of other persons in personal data is misguided as data privacy does not extinguish the interests in personal information of other entities.[51]

African countries in general, and Nigeria in particular, must come to terms with the present day realities of the online environment. The upsurge in the use of the internet, with the attendant proliferation of personal data, means more and more loss of control over personal data. It is, therefore, submitted that there is a sufficient basis for stronger 'rights-based' regimes to enhance data subjects' control over the processing of their personal information. This is a matter of dignity, human rights and fundamental freedom which must always prevail. The rest of the chapter will focus on the application of the rights-based approach based on a comparative analysis of specific focus areas in the Canadian and South African data privacy regimes.

6.3. The role of the constitution (Bill of Rights) in data privacy protection

There is no better way to advance a truly 'right-based' or 'an individual-centred' data privacy protection than by anchoring it in the constitution of a country. The Bill of Rights[52] contained in constitutions serves this useful purpose. Since the constitution is the basic law of a land, rights contained in the Bill of Rights enjoy an elevated status as they are constitutionally guaranteed and protected.[53] Indeed, Rouvroy and Poullet pointed out that '[t]he constitutional status given to Data Protection [in the EU] provides data

50 Chapter 2.

51 In fact, the scholar contends that '[data] privacy can foster trade and commerce, as it may enhance the trust of users in the business with which they are transacting'. Birnhack (n 47 above) 510.

52 Fombad observes that 'the fact that a constitution does not expressly refer to or use the term "Bill of rights" does not necessarily mean that it does not recognise and protect human rights: What is perhaps of more importance is whether a constitution contains provisions which do what a Bill of rights is supposed to do' CM Fombad 'African Bills of Rights in a comparative perspective' (2011) 17(1) *Fundamina* 35.

53 Dada pointed out that '[t]o concretize and energise human rights protection at national level, virtually all national constitutions embody human rights either in their preamble or substantive provisions.' JA Dada 'Human rights under the Nigerian Constitution: Issues and problems' (2012) 12(2) *International Journal of Humanities and Social Science* 33,

protection regime with a sort of constitutional privilege over competing legislative texts and allows for Constitutional control of its implementation respect by the Constitutional Courts.'[54] Thus, for a data privacy regime that seeks to be genuinely 'individual-centred', the first step is to entrench data privacy in the Bill of Rights of a country's constitution. This applies more for African countries as Fombad observes that 'Bills of Rights or provisions protecting human rights have particular importance in Africa because of the continent's poor human rights record dating particularly from the colonial period and probably even before then'.[55]

A data privacy regime based on the constitution not only establishes a negative obligation on the state not to unlawfully and unfairly process individuals' personal information, but also a positive obligation to empower individuals to exercise the right against the state and other entities.[56] It is, therefore, this researcher's view that, by establishing a nexus between data privacy and the Bill of Rights, the individual's rights and interests will be considered above any other interest of the data controller/responsible party.

Canada and South Africa have approached the constitutional entrenchment of data privacy differently. The Canadian Charter of Rights and Freedoms ('Canadian Charter'), which forms part of Canada's Constitution, does not explicitly provide for the right to privacy.[57] The right to information privacy is, however, read into other provisions in the Constitution, notably sections 7 and 8.[58] Thus, the courts have interpreted section 8 broadly and contextually.[59] Section 8 protects individuals against any form of unwarranted state interference with their reasonable expectation of privacy.[60] Similarly, section 7 has been

54 Rouvroy & Poullet (n 48 above) 71.
55 Fombad (n 52 above) 33.
56 See generally, FH Cate & R Litan 'Constitutional issues in information privacy' (2002) 9(1) *Michigan Telecommunications and Technology Law Review* 36-63. The commentators contend that '[t]he Constitution traditionally limits only actions by the government. However, as technologies give anyone the power to capture information, and create incentives for large private-sector databases that can then be accessed by the government, it is easy to question whether the constitutional distinction between public and private will retain the same significance.' 62. Their discussions are with respect to the US.
57 Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982 (Canadian Charter). Available at http://laws-lois.justice.gc.ca/eng/const/page-15.html (accessed 1 November 2015).
58 Canadian Charter (n 57 above).
59 Department of International Law, Permanent Council of the Organization of American States 'Comparative study: Data protection in the Americas' OEA/Ser.G CP/CAJP-3063/12, 3 April 2012. Available online at http://scm.oas.org/doc_public/ENGLISH/HIST_12/CP28327E04.doc (accessed 1 November 2015) 18.
60 Department of International Law (n 59 above) 19.

interpreted by the courts to provide residual protection to data privacy.[61] Both the Canadian Privacy Act and Personal Information Protection and Electronic Documents Act (PIPEDA), arguably, do not make explicit reference to the right to privacy under the Constitution.[62] They both state only that their objective is to foster privacy without referring to the Canadian Charter. Nevertheless, the Supreme Court of Canada has held that both Acts have quasi-constitutional status[63] which means they are not subject to the overriding provisions of other laws.[64] This has elevated the status of data privacy protection in Canada.

The Courts in South Africa, as in Canada, recognise the right to data privacy by reading in the *sui generis* protection in the provision of section 14 which guarantees privacy protection.[65] Unlike Canada, however, South Africa's approach is more specific and clearer for a number of reasons. Firstly, the right to privacy is explicitly provided in the South African Constitution so the courts and legal scholars merely uphold the right to data privacy (information privacy) as a sub-category of the right to privacy.[66] Secondly, the POPIA makes express reference to the right in the Constitution.[67] It is, therefore, safe to argue that the *sui generis* right to data privacy in Canada and South Africa has benefitted from the court's judicial activism.[68] Nevertheless, this may be problematic taking into consideration contemporary debates on data privacy protection. Firstly, the recent argument on data privacy is that it protects interests far beyond privacy interests in personal information. As noted in chapter two,[69] an assumption, therefore, that data

---

61 Department of International Law (n 59 above) 19.

62 PIPEDA, sec 3; Privacy Act, sec 2.

63 See *Lavigne v Canada (Office of the Commissioner of Official Languages)* (2002) 2 SCR 773. Available at http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1994/index.do (accessed 1 November 2015).

64 Even if they can be overridden by other laws, such overriding must be based on very clear and explicit provisions. See WN Eskridge 'Quasi-Constitutional law: Clear statement rules as constitutional lawmaking' (1992) 45*Vanderbilt Law Review* 593.

65 See Chapter 5 for more elaborate discussions.

66 See Chapter 5 for more elaborate discussions. See *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit* No 2001(1) SA 545 (CC).

67 POPIA, sec 2. In fact, it is further stated in the preamble of the Act that sec 14 of the South African Constitution provides for the right to privacy and 'the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.'

68 'Judicial activism is the view that the Supreme Court and other judges can and should creatively (re)interpret the texts of the Constitution and the laws in order to serve the judges' own visions regarding the needs of contemporary society. Judicial activism believes that judges assume a role as independent policy makers or independent "trustees" on behalf of society that goes beyond their traditional role as interpreters of the Constitution and laws.' See 'Judicial activism law & legal definition' http://definitions.uslegal.com/j/judicial-activism/ (accessed 1 November 2015).

69 See chapter 2 (2.6).

privacy is a sub-category of privacy will lead to an absurd situation where the courts will recognise violation of data privacy only in cases where they also constitute interference with privacy.[70] This is problematic considering that a processing activity such as the recording of personal information without anything more cannot, *prima facie*, constitute an interference with private life. Such an act is, however, data processing and falls within the scope of data privacy law.[71] Rodotà's view is apt in this regard as he argues that, for effective protection of individuals, data privacy as a fundamental right should not be considered as subordinate or subject to other rights.[72] Secondly, data privacy *stricto sensu* 'often does not handle private or sensitive data, but public and non-sensitive data'.[73]

One may hope only that, with time, more policymakers and legal scholars in Africa (and even Canada) will begin to recognise data privacy as a stand-alone right.[74] The approach of the EU and some European countries show insights in this regard. As stated in chapter two, the right to data privacy is now recognised as an independent right in this jurisdiction.[75] Data privacy is, thus, constitutionally recognised by the legislature and not by the benevolence of the judiciary. The approach of a few African countries is also worth mentioning. For example, the Constitution of Kenya[76] in sec 31(c), provides specifically for the right to protection of information, however, as a subset of the right to privacy. The

---

70 Lynskey (n 46 above) 569-597.

71 For eg, See the decision of the Court of Justice of the European Union (CJEU) in *Österreichischer Rundfunk and others* (2003) ECR I-4989 and analysis by Lynskey (n 46 above) 576

72 S Rodotà 'Data protection as a fundamental right' in S. Gutwirth *et al* (eds) *Reinventing data protection* (2009) 80

73 Van der Sloot (n 25 above) 308, such as names, telephone number etc.

74 Canadian scholars maintain that data privacy (information privacy) is part of the right to privacy. Their view is held on several grounds. Eg, Lisa Austin was of the view that one of the ways to protect privacy is by guaranteeing power of control over personal information. Her view in this regard was based on Alan Westin's seminal work which defined privacy in terms of power of control. See Westin (n 24 above). She further justifies her view by relying on Charles Fried's argument that privacy 'is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.' See L Austin 'Reviewing PIPEDA: Control, privacy and the limits of fair information practices' (2006) 44 *Canadian Business Law Journal* 24. Although, she criticised the idea of equating privacy with control, she does not, however, deny that control of personal information is a part of privacy.

75 Unlike the approaches of Canada and South Africa, the EU has given a more prominent role to data privacy in the constitution. De Hert & Gutwirth states that '[a]pparently, something new is happening at the constitutional level' as 'the constitutional lawmaker goes a step further and provide for an independent fundamental right.' De Hert & Gutwirth (n 18 above) 7.

76 The Constitution of Kenya (2010) available at http://www.kenyaembassy.com/pdfs/the%20constitution%20of%20kenya.pdf (accessed 1 November 2015).

Constitutions of Cape Verde[77] and Mozambique[78] is closer to the rights-based thesis proposed in this chapter. Article 42 of the Cape Verde's Constitution and article 71 of the Mozambique Constitution both provide for independent rights to protection of personal information separate from the right to privacy in their Bills of Rights. However, both provisions are limited only to personal information processed by computerised means. Recognition of the full value of data privacy will, no doubt, enhance data privacy protection and ensures that it is prioritised among other competing interests.

Nonetheless, Bergkamp seriously criticises the EU's approach and the approach of associating data privacy with rights which are constitutionally protected. He argues that:

> [a]n unfortunate consequence of including this right [data privacy] among truly fundamental rights, such as the prohibition of torture and slavery and the freedom of expression, is that the notion of fundamental right seriously devaluates, with adverse consequences for the respect for the core human rights.[79]

It is submitted that such an argument takes a narrow view of the threats which result from unlawful and unfair processing of personal information. It undermines the rights of individuals in the present day computing environment and ignores the substantial inequalities that exist between individuals and modern day data processors. Without a data privacy regime which is substantially rights-based, exploitation of data subjects will go unabated by public and private data controllers.

Although the Bill of Rights in the constitution plays a crucial role in the realisation of a rights-based approach to data privacy, it must be pointed out that reasonable restrictions can be placed on the right. Indeed Wheare observes that 'if a government is to be effective, few rights of its citizens can be stated in absolute form.'[80] It is, therefore, submitted that restrictions placed on the right to data privacy (and other rights in the Bill of Rights) must be construed narrowly and should not unnecessarily grant government agencies (and

---

77 The Constitution of the Republic of Mozambique (2004) revised in 2007 available at https://www.constituteproject.org/constitution/Mozambique_2007?lang=en (accessed 1 November 2015).

78 The Constitution of Cape Verde (1992) with amendments in 1999 available at https://www.constituteproject.org/constitution/Cape_Verde_1992?lang=en (accessed 1 November 2015).

79 Bergkamp (n 42 above) 33.

80 KC Wheare *Modern constitutions* (1966) 38. See also BB Lockwood *et al* 'Working paper for the committee of experts on limitation provisions' (1985) 7(1) *Human Rights Quarterly* 35

commercial entities) undue influence in the processing of the personal information of individuals.

6.4. Statutory protection of data privacy and the rights-based approach: Preliminary considerations

Quite a lot about the realisation of adequate protection of data privacy has to do with the quality of the statutory framework that is the data privacy law. The rest of the chapter will focus on particular aspects of a data privacy law and how it should be tailored so as to be in accordance with the right-based approach or truly individual-centred regime.

6.4.1. The law-making process

A comprehensive *sui generis* law is crucial for a regime that aspires to provide genuine protection of the data privacy right of individuals. In designing the law, three factors with rights-based implications, must be taken into consideration. Firstly, there is the motivation behind the law. Secondly, there is the membership of the law-making committee and, thirdly, there is the need for consultation with relevant stakeholders.

The motivation for the law will, without a doubt, have an influence on the subsequent provisions of the law. Laws with clear human rights motives will most likely adopt a rights-based approach. Conversely, laws with business objectives will also carry a business agenda. The Canadian Privacy Act, to a large extent, was motivated by human rights considerations.[81] Human rights consideration was, however, far from being the motive behind the PIPEDA, and this is reflected in subsequent provisions of the Act.[82] Berzins contends that '[i]ndustry Canada saw privacy protection as a key plank in its e-commerce strategy'.[83] In the preparatory process of the PIPEDA, undue considerations and concessions were given to the business community.[84] The South African POPIA, on the other hand, was motivated by human rights objectives although sufficient consideration was also given to other interests such as trade.[85] It may be safe to argue, nevertheless, that

81 See discussions in chapter 4.
82 See discussions in chapter 4. Eg, enforcement is generally lax and some provisions can be construed as giving undue advantage to businesses.
83 C Berzins 'Protecting personal information in Canada's private sector: The price of Consensus building' (2002) 27 *Queen's Law Journal* 625.
84 Berzins (n 83 above) 625
85 See SALRC (n 41 above) para 1.2.1-1.2.7.

human rights motives were given priority. This also reflects in subsequent provisions of the Act.

With regard to the nature of the members of the committee, since data privacy law mainly involves a mixture of IT and human rights, the design process of a rights-based law should comprise of experts in both fields. The influence of members of the law-making committee on the final draft of the law cannot be overemphasised. Similarly, formulating a data privacy code that is rights-based should also involve sufficient consultation with those who will be affected by the provisions of the law. In this regard, a researcher observes that:

> [o]rdinarily, public consultations in the legislative process generate debates about the need or otherwise of data privacy laws, their contents, enforcement, etc., and in the course of that stimulates interests and awareness in these laws to the public. Concomitantly, they facilitate implementation of data privacy laws once enacted.[86]

Thus, public consultation will ensure that the essential values which the law seeks to promote are easily ascertained from relevant stakeholders. These issues will be discussed in greater detail in the next chapter.

6.4.2. Purposes/objectives of the law

According to Bygrave, 'data privacy law has long been afflicted by [the] absence of clarity over its aims and conceptual foundation.'[87] Accordingly, determining the exact objective of a data privacy instrument is difficult. Contemporary debates on objectives of data privacy law are focused on the conflicts in the objectives of data privacy. In many cases, data privacy objectives are usually overshadowed by other objectives. Schartum describes the practical implication of these conflicts by stating that the fact that data privacy objectives are usually overshadowed by other objectives does not imply the disappearance of data privacy.[88]

> Rather, the effect of data protection is weakened in the sense that one or more exceptions to the principles of data protection are introduced. Major section of the data protection debate concerns the degree to which individual rights and guarantees should be overshadowed.[89]

---

86 Makulilo Dr. Jur. Thesis (n 4 above) 276.
87 LA Bygrave *Data privacy law: An international perspective* (2014) 117.
88 Schartum (n 34 above) 5.
89 Schartum (n 34 above) 5-6.

In this researcher's view, a data privacy instrument that gives priority to human rights should be clearly discerned from the objective/purposes of the law.[90] Thus, a data privacy instrument that is rights-based must be formulated in a way that promotes data privacy rights of individuals as narrowly construed. Both the Canadian Privacy Act and the PIPEDA have shown that safeguarding privacy is a core objective.[91] Yet, from the title of the PIPEDA, it can be discerned that greater emphasis is paid to the business objective, probably at the expense of safeguarding privacy.[92] The title unequivocally states that the Act is to 'support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances.'[93] This shows a market-based or interest-driven data privacy law. The South African POPIA, like both Canadian data privacy laws, also provides for safeguarding privacy as a basic objective.[94] There are, however, still other interests the POPIA seek to foster outside of privacy.[95] A careful look at section 2 of the POPIA, apart from being explicit, shows more focus on the privacy rights of individuals, which, in this reseracher's view, is insightful for a rights-based regime. It must, however, be pointed out that safeguarding privacy, which these laws uphold as a primary objective, is problematic. This is because, according to Bygrave, '[w]hile privacy does occupy a central place in data privacy law, it is not the sole concern of such legislation.'[96] He further stressed that '[l]egislation on data privacy serves a multiplicity of interests, which in some cases extend well beyond traditional conceptualizations of privacy.'[97] These interests range from privacy, dignity, liberty, integrity and so on. Perhaps one may argue that rather that pin the objective of data privacy law down to a particular interest, stating that the law is mainly for the 'protection of fundamental rights and freedom' of individuals is a better approach.[98] Yet, it may still be argued that this approach may suffer from obscurity and ambiguity which laws should generally avoid. It is submitted that, notwithstanding this, that is a better approach.

---

90 Although Bygrave rightly acknowledges that some data privacy laws do not even contain an object clause probably because of the obscurity of the aim of data privacy law. Examples given by the author are the UK and Denmark's data privacy laws. Bygrave (n 87 above) 118.

91 Privacy Act, sec 2; PIPEDA, sec 3.

92 Privacy Act, sec 2; PIPEDA, sec 3.

93 Privacy Act, sec 2; PIPEDA, sec 3.

94 POPIA, sec 2.

95 See discussion in chapter 5.

96 Bygrave (n 87 above) 119.

97 Bygrave (n 87 above) 119.

98 See the draft EU Regulation.

6.4.3. The scope of the law: An evaluation of Schwartz and Solove's proposal and the rights-based approach

An important question with respect to a discussion on the scope of a data privacy instrument is: 'how can it be formulated and applied to ensure greater protection for individuals with respect to the processing of their personal information?' As noted in chapters four and five, a discussion on the scope of a data privacy law will focus on scope with regard to the type of data, type of data processing, and the sectors covered. The last two are not really the subject of contemporary debates. The scope with regard to the type of data is what is controversial, and it will be the focus of this section of the chapter. Generally, the jurisdiction of a data privacy law is triggered whenever there is personal information as narrowly construed under the law.[99] It is usually argued that the range of personal information covered in a data privacy law goes to show the scope of protection granted to individuals. Seen in this light, the wider the information covered, the more protection individuals have with regard to the processing of their data. Thus, Lindsay rightly points out that 'the kinds of information falling within the scope of information privacy laws would likely be much greater under a rights-based approach than under a market-based approach.'[100] In another work, Lindsay and Ricketson noted that '[l]aws that adopt a rights-based approach to data protection appear to have a broader scope [with respect to personal information] than laws with an 'interest-based' perspective.'[101] Van der Sloot states as a rationale for the increasing broadening of the scope of data privacy law with regard to the type of data. In her words, '[t]o cope with the fact that personal data are less and less linked to the individual subject, the definition of personal data has been widened and broadened over time.'[102]

Normally, data privacy laws are applicable to information that *relates to* or *identifies* or is capable of *identifying* an individual.[103] The recent trend is to couch data privacy laws in a

---

99 De Hert & Papakonstantinou (n 28 above) 132; Bygrave (n 87 above) 129.

100 D Lindsay 'An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law' (2005) 29 *Melbourne University Law Review* 177.

101 Lindsay & Ricketson (n 26 above) 142.

102 Van der Sloot (n 25 above) 309.

103 Some laws combine all in the definition. Eg, see draft EU Regulation and EU Directive. Bygrave observes, based on an analysis of arts 2(a) of the CoE Convention 108; para 1(b) of the OECD Guidelines and art 2 of the EU Directive that two cumulative conditions for data to be 'personal' exists. Firstly, data must relate to an individual and secondly, it must enable the identification of such person. Nevertheless, he went further to state that 'it may not be appropriate to talk of two separate (although cumulative) conditions for making data 'personal'; the first condition can be embraced by the second in

manner that covers the remotest possibility of identification depicting an increasing scope of personal information covered. Thus, once information is capable of identifying an individual, data privacy laws are applicable, and it is immaterial whether such information does not actually identify an individual.[104] In this regard, Bygrave notes that:

> [i]t bears emphasis that, at least for some laws, such as the DPD, what is of legal importance is the capability or potential of identification rather than the actual achievement of identification. Hence data will not fail to be personal merely because the data controller refrains from linking it to a particular person. [105]

Nevertheless, some laws, like the EU data privacy codes, are applicable to both 'identified' and 'identifiable' information.[106] It is submitted that including both is unnecessary as information that is capable of identifying an individual has a broad scope and covers information that identifies such individual. Nevertheless, one may argue that a data privacy instrument that applies to only *identifiable* information forecloses *identified* information. That argument will, in this researcher's view, be stretching imagination too far. From this brief analysis, three kinds information are crucial for data privacy law: identified, identifiable and non-identifiable information. While data privacy laws apply primarily to the first two, they do not apply to the last.

The Canadian Privacy Act, even though applicable to 'identifiable information', has a narrow scope because it, arguably, applies to information in a recorded form only.[107] On the other hand, the PIPEDA applies to 'information about an identifiable individual'.[108]

---

the sense that data will normally relate to, or concern, a person if it enables the person's identification.' Bygrave (n 87 above) 129.

104 Lynskey noted that 'data protection rules apply where identification is possible, regardless of whether or not identification occurs.' Lynskey (n 46 above) 584.

105 At least, this is so for the EU models of data privacy law. Bygrave (n 87 above) 132.

106 Art 2 of the EU Directive provides that "'personal data' shall mean any information relating to an identified or identifiable natural person'. It further defines and identifiable person as 'one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.' On the other hand art 4 of the draft EU Regulation provides that 'personal data means any information relating to a data subject.' A data subject on the other hand is defined in the same provision as 'an *identified* natural person or a natural person who *can be identified*, directly or indirectly, ***by means reasonably likely*** to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.' The draft EU regulation, in its truly rights-based character, has shown, from the definition, the increasing scope of data privacy laws by providing that more conditions that the natural person: a) can be identified; b) directly or indirectly c) by means reasonably likely.

107 Privacy Act, sec 3. See discussions on this issue in chapter 4.

108 PIPEDA, sec 2. The definition does not include the name, title or business address or telephone number of an employee of an organisation.

The Canadian PIPEDA goes a step further than the EU Directive by dropping 'identified' information.[109] The South African POPIA's approach is also similar to the Canadian PIPEDA in that it is also applicable to 'information relating to an identifiable…person'.[110] From the forgoing, two important points can be discerned. Firstly, identifiability, which is 'the potential of data to enable the identification of a person', [111] is the crux of the scope of the law with regard to type of data[112] and, secondly, the Canadian and South African data privacy laws have largely followed the EU and its approach of increasingly expanding the scope of identifiability with regard to personal information. This approach is what has been described by Schwartz and Solove as 'the expansionist approach' and, according to them, is 'more in tune with technology' and 'it has exerted significant international influence.'[113] In contrast to the EU archetypes, the US tends to reduce the scope of personal information in its patchwork data privacy laws. This approach, according to Schwartz and Solove, is 'the US reductionist approach.'[114] In the reductionist approach, 'the tendency is to consider PII [personal identifiable information or personal information] as being only that personal data that has been specifically associated with a specific person.'[115] In other words, the US's approach considers only data that already *identifies* and not that which is *capable of identifying* an individual as subject of protection.

Schwartz and Solove, have criticised the EU expansionist approach as being too wide as it treats 'identified and identifiable data as equivalent'.[116] They also argued against the US reductionist approach as it 'protects only identified data, and thereby leaves too much personal information without legal protection.'[117] In the light of these criticisms, they

---

109 PM Schwartz & DJ Solove 'The PII problem: Privacy and the new concept of personally identifiable information' (2011) 86 *Newyork University Law Review* 1875. For more discussions on the expansionist approach of the Canadian PIPEDA, see 1875-1876.

110 POPIA, sec 1.

111 Bygrave (n 87 above) 130. The scholar defines the concept of identifiability as 'the ability to distinguish a person from others by linking him or her to pre-collected information of some kind.'

112 For more in-depth analysis on the concept of identifiability, see Bygrave (n 87 above) 129-140.

113 Schwartz & Solove (n 105 above)1875.

114 Schwartz & Solove (n 105 above)1875.

115 Schwartz & Solove (n 105 above)1817.

116 Schwartz & Solove (n 105 above) 1817.They further contend that '[n]otwithstanding its widespread adoption in other international documents, the European Union's expansionist approach is flawed because it treats data about identifiable and identified persons as conceptually equivalent. The difficulty is that there is a broad continuum of identifiable information that includes different kinds of anonymous or pseudonymous information. Different levels of effort will be required to identify information, and varying risks are associated with the possible identification of data. To place all such data into the same conceptual category as data that currently relate to an identified person is a blunt approach.' (n 103 above)1876.

117 Schwartz & Solove (n 109 above) 1817. The data privacy scholars explained the implications of the expansionist and reductionist understanding of personal information. They pointed out that 'PII is a

developed a standard for personal information called the *PII 2.0*, which is based on 'identification in terms of risk level' [118] otherwise called the 'harm-based approach'.[119] The approach, according to them, 'permits tailored legal protections built around different levels of risk to individuals.'[120] In applying the standard, they categorised personal information into *identified, identifiable* and *non-identifiable*.[121] The essence of this categorisation is so as to vary the obligations or FIPs applicable in the case of each category because 'the continuum of risk is different for these categories.'[122] All the FIPs will, therefore, apply in cases of personal information that identifies an individual, and some FIPs will apply in instances where the information is merely capable of identifying a person. In the case of non-identifiable information, no FIP will be applicable.

The learned scholars' proposal looks convincing. It is, however, submitted that certain preliminary issues with regard to personal information and the threats that come with its processing must be properly appreciated. In this researcher's view, personal information, whether "capable of identifying" or "identifies" an individual is all the same provided it relates to an individual. The assumption under data privacy law is that the protection granted to individuals should not be based on the probability of identification. Once information relates to a data subject, the probability or ease of identification does not in any way reduce the risk that individuals can be exposed to.[123] In other words, the ease of

---

challenging conceptual issue at the heart of any system of regulating privacy in the Information Age. If PII is defined too narrowly, then it will fail to protect privacy in light of modern technologies involving data mining and behavioural marketing. Technology will thus make privacy law irrelevant and obsolete. On the other hand, if PII is defined too broadly, then it could encompass too much information and threaten to transform privacy law into a cumbersome and unworkable regulation of nearly all information. Privacy law must have coherent boundaries, which adequately protect privacy and which can be flexible and evolving.' (n 109 above) 1827

118 Schwartz & Solove (n 109 above) 1879. This also seems to be in line with Austin's view that '"personal information" should receive a broad interpretation and the question of when information is "identifiable" should be answered utilizing a re-identification of risk approach. Both of these are matters of statutory interpretation.' Austin (n 74 above) 52.

119 PM Schwartz & DJ Solove 'Reconciling personal information in the United States and European Union' (2014) 102 *California Law Review* 912.

120 Schwartz & Solove (n 109 above) 1877. According to the scholars, the approach 'also represents a path forward, one that avoids both the United States' reductionist view of PII, and the European Union's expansionist view.' 1817.

121 Schwartz & Solove (n 109 above) 1877.

122 Schwartz & Solove (n 109 above) 1877.

123 Both scholars seem to admit this fact in a part of their paper entitled "possible objection" (n 109 above 1883). The argument given there is, however, still unconvincing. They contend that '[i]n our view…computer science is developing metrics that are suitable for just this task.' i.e, the task of determining identifiably. They further argued that the standard proposed 'will be as workable as the law's recourse to standards in other areas, such as the concept of "reasonable" behaviour in negligence law, or that of "access or acquisition of information" in data breach notification law".' It is my view that such a context specific application will still be a gateway for data controllers and responsible

identification that certain information presents does not lower the risk thresholds that more difficult identifiable information presents. Identification is identification, and once information can identify a person, irrespective of level of effort involved, individuals ought to be *fully* protected by data privacy law.[124] In this regard, Lynskey argues that data privacy law 'apply where identification is possible regardless of whether or not identification occurs.'[125] This is the whole idea of a rights-based approach which advocates a broad interpretation of personal information.

Attempts to justify the proposal are not convincing. Schwartz and Solove have argued that traces of the application of their proposal can be found in the categorisation of sensitive and non-sensitive personal data (especially in the EU regime).[126] Nevertheless, it is submitted that such categorisation does not lower the 'high-level' protection given to personal data. Rather, it heightens the protection on sensitive data without, in any way, lowering the threshold of protection for non-sensitive information. All the FIPs are, therefore, applicable to both sensitive and non-sensitive personal data.

The proposal of Schwartz and Solove may be a reflection of attitude of the US (and its scholars) towards data privacy where efforts are continuously being made to weaken privacy protection at various levels, even though, they rightly 'reject[ed] the idea that privacy law should abandon the concept of PII Personally Identifiable Information or personal information' because, according to them, '[i]f it did so, privacy law would be left without a means for establishing coherent boundaries on necessary regulation.'[127] Schwartz and Solove are, however, more concerned about developing a standard that is workable for both the EU and US at the expense of individual's data privacy. Their standard looks to how companies can benefit from the processing of an individual's personal data. It is submitted that such a proposal may lower the high-level of data privacy protection which the right-based approach seeks to elicit. In essence, personal information must be construed as widely as possible irrespective of a theoretical anticipation of the kind of risk an individual may be exposed to once he/she is identified. This researcher's

---

parties to avoid certain obligation which may be tantamount to lowering data privacy standards across the world.

124 See Bygrave's analysis. (n 87 above) 130-131.

125 Lynskey (n 46 above) 584.

126 Schwartz & Solove (n 119 above) 913. They argue that '[a]s a larger point, the concept of sensitive data shows how the European Union already supports different categories of data with different levels of protection.'

127 Schwartz & Solove (n 109 above) 1865.

view is a result of the complex and sophisticated nature of modern data processing which even the scholars have admitted on several occasions.[128] Even if there should be discrimination between certain categories of personal information, such discrimination should not generally lower the threshold of protection.

6.4.4. Exemptions and exclusions from the scope of the law

An important question in the context of a discussion on exclusions and exemptions is what should be the attitude of a truly rights-based regime towards exclusion and exemptions?[129] The SALRC gives us guidance in this regard. The commission pointed out that '[s]tatutory exemptions from particular principles are to be preferred over exclusion from the Act of an entire class of responsible party or information.'[130] Exemptions, therefore, from particular principles are *necessarily evils* in rights-based regime which are preferred over exclusions from the law generally.

The main exclusions from the scope of the laws are those for personal, journalistic, artistic and law enforcement purposes. These exclusions are provided for under the Canadian Privacy Act and PIPEDA, and under the South African POPIA.[131] Under these laws in addition, powers are given to certain authorities (usually, the DPAs) to exempt a certain category of persons from the provisions of the Act.[132] These are mainly for public purposes, example for law enforcement, prevention and detection of crime and security of life and property. In this researcher's view, a rights-based approach will permit these exemptions and exclusions. They must, however, be narrowly construed by the enforcement institution. In this case, the data privacy right of a data subject must be put on an imaginary scale with the purpose of such exemption or exclusion. It must, however, be emphasised that it is important that rights are prioritised.

---

128 They stated that 'computer science has shown that in many circumstances, non-PII can be linked to individuals, and that de-identified data can be re-identified.' (n 109 above) 1814. They further noted that 'PII and non-PII are thus not immutable categories, and there is a risk that information deemed non-PII at one time can be transformed into PII at a later junction.' (n 109 above) 1814. In extending their argument in this regard, it is submitted that with advances in technology, information that is capable of identifying an individual could as well be information that has identified an individual.

129 Both will be used interchangeably in this part

130 SALRC (n 41 above) para 4.4.2. See also Rodotà (n 72 above) 80-81.

131 PIPEDA, sec 4 PIPEDA; POPIA, sec 6.

132 Privacy Act, sec 18(1). POPIA, sec 37.

A very controversial exclusion in many data privacy codes is exclusion for 'purely personal or household activity'.[133] This has been the subject of much academic debate recently. The main issue is: is this category of exclusion justifiable in the face of remarkable advances in technology where an individual can process a vast amount of personal information with the smallest of devices? In this case, such an individual can easily argue that such processing is for personal purposes. This exclusion, which is contained in the EU Directive and is still retained in the draft EU Regulation, has been severely criticised.[134] Kotschy, for example, observes that:

> [t]his exemption goes back to the 1990s, when the possibilities for private individuals to process data about others were limited by existing technical and behavioural standards. The internet plus social media plus camera on mobile phones has drastically changed the way that private persons use electronic means to disseminate data, especially pictures, not only about themselves but also about others. In this new environment the right balance between the freedom of the individual to make use of all available facilities and the right of others to adequate protection of their data is unhinged. [135]

Perhaps these criticisms are what made the draft EU Regulation to explicitly provide, in recital 15, that 'the Regulation should not apply to processing of personal data …which are exclusively personal or domestic…*without any gainful interest and thus without any connection with a professional or commercial activity'*[136] But, then, this does not solve the problem, as individuals may still process personal data without any profit-making motive in a way that may affect the rights of other individuals (for example, bloggers). Roos suggests that the exclusion applies only 'as long as the individual collecting the information does not place it on the internet and make it available to more persons than his or her family!'[137] The European Commission, however, was of the view that 'the best way to address the problem is to regulate the services that such ordinary users rely on.'[138] For

---

133 PIPEDA, sec 4(2)(b); POPIA, sec 6(1)(a).

134 EU Directive, art 3(2); draft EU Regulation, art 2(2)(d). It was observed that 'there is the danger, on the one hand, of exempting from the law, activities that directly impact on privacy and data protection; and on the other hand, of applying "heavy" rules, designed to regulate (presumably) well-organised institutions, to simple actions carried out by ordinary individuals as part of their everyday activities.' See European Commission 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological development' (2010) final report. para 24 Available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf (accessed 1 November 2015).

135 W Kotschy 'The proposal for a new General Data Protection Regulation – problems solved? (2014) 4(4) *International Data Privacy Law* 277.

136 (Emphasis added) draft EU Regulation.

137 A Roos 'Personal data protection in New Zealand: Lessons for South Africa? (2008) 11 *Potchefstroom Electronic Law Journal* 79

138 European Commission (n 134 above) para 35.

example, the social networking sites and the sites hosting the blog should be 'made to provide default settings for their sites and services and tools that are privacy friendly.'[139] There could also be strict supervision of these services to ensure that they strictly comply with the FIPs. These issues will be considered later.

6.5. The fair information principles (FIPs), rights of data subjects and the rights-based approach

6.5.1. Some preliminary comments on the FIPs

Without a doubt, the FIPs in any data privacy instrument are established for the major purpose of advancing the rights, or protecting the interests of a data subject. As a consequence, they are arguably 'individual-centred'. Nevertheless, in line with the proposal of a rights-based data privacy regime, the FIPs must go further by doing two things. Firstly, the individual and his/her interests must be accorded topmost priority and, secondly, they should contain very few exceptions or at best, specific exceptions, not general, sweeping exemptions.[140] It may seem that the approach proposed in this chapter is oblivious of other interests in individual's personal information. This is, however, not the case. The point must be stressed that a rights-based approach is not unmindful of other interests in individuals' personal information. After all, even the individual may, in certain circumstances, need his/her personal information to be processed.[141] Human rights of the data subject must, however, always prevail.

In essence, the FIPs that are truly 'individual-centred' (by protecting them from unfair processing) have largely to empower individuals to exercise control of their personal data. Some commentators, however, seem to suggest otherwise. Cate, for example, argues that a regime that is 'individual-centred' does not necessarily entail granting a data subject maximum control of his/her personal information.[142] He stressed that many of the FIPs have been adopted to reflect a distinct goal of data protection as empowering individuals to

139 European Commission (n 134 above) para 35.
140 SALRC (n 41 above) para 4.4.2.
141 I have discussed the importance of the processing of individuals' own personal data in chapter 2 above.
142 FH Cate 'The failure of fair information practice principles' in JK Win (ed) *Consumer protection in the age of the information Economy* (2006). Similarly, Austin seems to be arguing that control is neither necessary nor sufficient for the protection of privacy. See LM Austin 'Privacy and the Question of technology' (2003) 22 *Law & Philosophy* 125.

exercise control over their personal information as opposed to protecting them from unfair or harmful use of their information.[143] In his words,

> [t]he greatest failure of FIPPS [FIPs] as applied today is the substitution of maximizing consumer [individuals] choice [power of control] for the original goal of protecting [data] privacy while permitting data flows. As a result, the energy of data processors, legislators, and enforcement authorities has been squandered on notices and often meaningless consent opportunities, rather than enhancing privacy. *Compliance with data protection laws is increasingly focused on providing required notices in proper form and at the right time, rather than on ensuring personal information is protected.* [Emphasis supplied]

The scholar further contends that the control-based system of data privacy law merely concentrates on the procedural principles at the expense of the substantive rules.[144] Two major examples of procedural principles are the provisions on consent and notices. Cate, therefore, argues that a strict requirement for procedural objective seems to overshadow the substantive objective which is the protection of individuals' data privacy rights.[145] In this researcher's view, there is no basis to separate both objectives of data privacy law which is one of the essences of a rights-based approach. Enhancing control, it is submitted, will foster data privacy rights by preventing unfair and harmful processing. Thus, the procedural requirement is for the purpose of realising the substantive objectives of data privacy. Both enhancing control and protecting individuals from unfair and harmful data processing are geared towards realising the adequate protection of data privacy.[146]

Another issue with regard to the FIPs which has a direct bearing on the rights-based approach proposed in this chapter is whether they (the FIPs) need to be overhauled. This issue is provoked by the contention that the FIPs were formed more than thirty years ago when the level of data processing was incomparable to what exists today. Nevertheless,

---

143 Cate (n 142 above) 14.
144 Cate (n 142 above) 14.
145 Cate (n 142 above) 14.
146 Yet another criticism of control as the basis of data privacy (and the rights-based approach) is that strenuously canvassed by Lisa Austin. She argues that, although control may provide privacy protection, equating control with data privacy as a definition matter is not convincing. She further claims that 'control' is not a basic condition for privacy protection, as individuals may be provided with control and yet still gives up their privacy. Similarly, she contends that organisations may choose to respect (data) privacy even when individuals do not have power of control. Her conclusion was that 'providing control over personal information does not necessarily ensure that individuals have informational privacy and providing no control does not necessarily entail a lack of informational privacy.' Austin (n 74 above) 24-25. Nevertheless, even she admitted that control over personal information may protect a broader set of value beyond privacy. This support the argument canvassed in this thesis that, although data privacy promotes privacy values, it goes beyond mere privacy protection.

Kotschy, relying on 'the outcome of the public consultation initiated by the EU Commission in the course of launching the project of the reform package',[147] contends that nobody has been able to prove convincingly that the principles need to be overhauled.[148] This is because '[m]ore than 30 years of practical application have proven these principles to be sound.'[149] A similar observation was also made by the expert group responsible for revising the OECD Guidelines in 2013.[150] The expert group was of the view that 'the balance reflected in the eight basic principles of Part Two of the 1980 Guidelines remains generally sound and should be maintained.'[151] Thus, the principles 'have stood the test of time'.[152] A principle-based approach, which is adopted by most data privacy codes, is also consistent with the demands of modern data processing challenges. Oyetayo rightly contends that a principled-based regulation is effective 'because of [its] flexibility, support for regulatory efficiency and the development of a good compliance culture amongst the regulated.'[153]

Although it is widely acknowledged that the FIPs still provide sound data privacy protection, there is still room for improvement to strengthen them further and ensure that individuals are indeed placed at the centre of data privacy protection. This is in tandem with my proposal for a rights-based data privacy regime. In this light, therefore, it is submitted that a rights-based regime should place increasingly detailed and specific

147 See Explanatory Memorandum of the proposed General Data Protection Regulation, context of the Proposal, COM (2012) 11 final, 2. Also at http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011 (accessed 1 November 2015).

148 Kotschy (n 135 above) 277.

149 Kotschy (n 135 above) 277. See also Art 29 Data Protection Working Party 'The future of privacy; Joint contribution of the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' WP 168 (2009) 3. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (accessed 1 November 2015).

150 Bygrave (n 87 above) 44.

151 See OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (accessed 1 November 2015). The eight principles referred to are collection limitation, data quality, purpose specification, use limitation, security safeguard, openness, individual participation, and accountability principles.

152 The European Commission was of the view that '[t]he basic data protection principles, rules and criteria, as developed in Europe by the COE and the EU, and as also broadly endorsed globally, in particular by the OECD, as such, have stood the test of time, even if they may need strengthening in some respects. It is a testimony to their wide acceptance that they are increasingly adopted as the basis for legislation in many parts of the world, including Asia and Africa.' European Commission (n 134 above) para 15.

153 Her discussion was, however, not on data privacy but on insurance. Y Oyetayo 'Principles based regulations: A model for legal reform in the Nigerian insurance industry' (2015) 59(1) *Journal of African Law* 64.

obligations on data controllers (or responsible parties) and grant data subjects more 'subjective' rights over their personal information processing.[154]

6.5.2. Increasingly detailed and specific obligations on data controllers

A rights-based data privacy regime should place increased obligations on entities that process an individual's personal information.[155] This is consistent with an added emphasis on the individual and his/her interest. The recent trend in contemporary data privacy codes is, thus, to provide elaborate provisions regarding the obligations of data controllers. This depicts a movement in the provisions of the FIPs from mere administrative principles of good governance to human rights principles.[156] The proposal for imposing more obligations on data controllers may, *prima facie*, seem to place an onerous task on businesses thereby discouraging the free flow of information.[157] Quite the opposite is the case for two reasons. Firstly, contrary to the prevailing assumption that more incentives need to be put in place to encourage data flow (in the form of less onerous obligations on data controllers), it is submitted that the current value of personal information makes the need for further incentives to encourage data flow unnecessary.[158] Secondly, detailed obligations or duties will guide controllers towards fulfilling their legal obligations thereby providing better services for data subjects in an atmosphere of trust and confidence.

Generally, eight principles of data privacy are recognised under international data privacy law. They are: processing limitation (or limitation of collection), data quality, purpose specification, use limitation, security safeguard, openness, individual participation, and accountability.[159] There are still other additional obligations on data controllers, such as extra protection for sensitive data and so on. The Canadian Privacy Act does not

---

154 In line with the approach of the draft EU Regulation. See general discussion in Van der Sloot (n 25 above). See also De Hert & Papakonstantinou (n 28 above).

155 Van der Sloot (n 25 above) 309.

156 Van der Sloot (n 25 above) 318.

157 Indeed, Flaherty observes that '[n]either government nor private sector really likes the privacy business…because it gets in the way of their continuing to do business as usual with personal information.' Quoted from Schartum (n 34 above) 4. Cavoukian also argued that more obligations are not a burden to businesses. See A Cavoukian 'Privacy by design in law, policy and practice: A white paper for regulators, decision makers and policy makers' available at https://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf (accessed 1 November 2015) 8.

158 Indeed, Bernal has been able to successfully show through various case studies that '[i]n the online world as it exists now, it does not seem that data flow needs much encouragement'. Bernal (n 1 above) 223.

159 These principles are in essence based on the principles contained in the OECD Guidelines.

coherently outline the obligations of a government institution.[160] Also, very limited obligations are imposed on government institutions. As observed earlier,[161] the main obligations in the Privacy Act are to comply with the processing limitation,[162] purpose specification,[163] use limitation[164] and data quality[165] principles. The obligation to delete personal information is also narrowly provided for.[166] Similarly, the Canadian Privacy Act provides for the retention of personal information so as to enable data subjects to exercise their rights of access.[167] Most of the obligations are, however, extremely narrow as they are applicable only where information is collected for 'administrative purposes'.[168] On the other hand, the PIPEDA requires all organisations to comply with FIPs in the schedule of the Act.[169] A cursory look at the PIPEDA shows that more detailed obligations are imposed on organisations that fall within its scope. The obligations are to comply with the principles of accountability (which includes appointing a data protection officer and liability for transfer to 3rd parties); identifying purposes; obtaining consent; limiting collection; use limitation; data quality (accuracy); security safeguards; openness; access and challenging compliance.[170] Despite its obvious economic agenda,[171] the PIPEDA gets closer to being rights-based than the Privacy Act in terms of imposing increasingly detailed and specific obligations on data controllers. Like the Privacy Act, however, it does not impose an obligation to provide special protection for sensitive personal information.[172]

Another major weakness of the PIPEDA which impacts upon the thesis of a *genuine* rights-based data privacy regime is section 5(3) which allows organisations to process individuals' personal information 'for purposes that a reasonable person would consider

---

160 See chapter 4 above for more elaborate discussion.
161 Chapter 4.
162 Privacy Act, sec 5(1).
163 Privacy Act, sec 4 & sec 5(2).
164 Privacy Act, sec 4 & sec 7.
165 Privacy Act, sec 6(2).
166 Privacy Act, sec 6(3).
167 Privacy Act, sec 6(1).
168 Privacy Act, sec 6(1).
169 PIPEDA, sec 5.
170 PIPEDA, sec 5. Schedule 1.
171 Which can be discerned from even the objective of the Act.
172 Nevertheless, some of the principles that are provided for stipulate a higher level of care for sensitive information. Eg, principle 7 which is on security safeguards provides in sec 4.7.2 that '[t]he nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.' See also clause 4.3.4 which provides for different levels of consent depending on the sensitivity of personal information.

are appropriate in the circumstances.' This provision, in this researcher's view, grants businesses the power to process personal information even without consent and other legitimizing grounds, provided such processing is considered 'appropriate'. Unfortunately, the PIPEDA neither defines nor explains what 'a reasonable person would consider…appropriate.' The provision will, therefore, serve as a means for data controllers to avoid their obligations.

Unlike both the Canadian Privacy Act and the PIPEDA, the South African POPIA is more in line with the proposal for a genuine rights-based approach. Firstly, the obligations (FIPs) are provided as substantial provisions in the Act, similar to the EU Directive and draft EU Regulation. Secondly, the POPIA contains very detailed provisions explaining the obligations of the responsible party.[173] Thirdly, responsible parties who fail to comply with these numerous obligations face severe sanctions.[174] The POPIA requires responsible parties to comply with eight broad conditions for lawful processing namely, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. It is noteworthy that within each of these conditions further obligations are imposed on responsible parties. For example, the condition of openness also includes the requirement that documentation must be kept and that notification must be given to the data subject when collecting his/her personal information.[175] Similarly, the data subject participation condition includes the provision that access must be given to personal information and that correction of such information must be allowed. What is more, several other obligations are imposed on responsible parties, such as rules on sensitive data processing, processing of children's information and the requirement of prior authorisation.

Two principles which place heavy obligations on data controllers, and are indeed crucial in a right-based data privacy regime, are the accountability and safeguards principles. Both are sufficiently provided for under both the Canadian PIPEDA and the South African POPIA. While the accountability principle holds data processors accountable for compliance with all the other principles, the safeguards principle requires them to ensure that appropriate security measures are put in place to secure personal information under their control. Accountability under the PIPEDA includes the obligation to appoint an

173 From secs 8-25. Several other provisions in the Act give a vivid elucidation of other obligations of data subjects.
174 POPIA, chapter 11 generally.
175 POPIA, secs 17 &18.

individual who should ensure compliance with the Act.[176] In addition, it is explicitly provided under the PIPEDA that an organisation is responsible for personal information transferred to third parties.[177] It is submitted that the scope of accountability under the POPIA is narrower when compared to the PIPEDA.[178]

6.5.3. More subjective rights for data subjects

Legal scholars have, over the years, stressed the importance of the rights of data subjects in a data privacy system. Greenleaf rightly points out that data privacy, like copyright, is a 'bundle of specific rights' benefiting data subjects.[179] Zanfir also expresses the view that 'the rights of the data subject are prerogatives which allow the individual to control the way in which his or her personal data are processed, regardless of the legal basis of the processing.'[180] In line with our proposed rights-based regime, thus, a data privacy instrument should contain more (strengthened) rights for the data subject, and such rights must be well-expressed so as to prevent unnecessary conjecture by desperate data controllers. Indeed, it has been noted that 'well expressed rights could support and empower individuals themselves and help them to find ways to get their concerns across.'[181] For the 'rights to be effective, however, individuals themselves need to acknowledge, on one hand, the risks entailed by data processing and the digital storage of personal data, and, on the other hand, the existence of their rights and the means to exercise them.'[182] This, in the researcher's, invokes the moral duty of individuals toward their own data privacy which will be discussed subsequently.

Under the Canadian Privacy Act, the main rights provided are the right of access and right of correction.[183] Unlike the Privacy Act, the PIPEDA does not explicitly set out rights of data subjects. This depicts a commercially-driven legislation.[184] The South African POPIA, on the other hand, has introduced a paradigm-shift in the provision on subjective

176 PIPEDA, clause 4.1.1 of schedule 1.
177 PIPEDA, clause 4.1.3 schedule 1. Similarly, clause 4.1.4 provides that an organisation must implement policies and practices to give effect to the other principles in the Act.
178 PIPEDA, sec 8.
179 Greenleaf (n 5 above) 5-6.
180 G Zanfir 'Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law' in S Gutwirth *et al* (eds) *Reloading data protection: Multidisciplinary insights and contemporary challenges* (2014) 248.
181 Bernal 2014 (n 1 above) 232.
182 G Zanfir 'The rights of persons regarding personal data protection' unpublished PhD thesis, University of Craiova, 2013 18.
183 Privacy Act, sec 12(2)(a) & (b).
184 See generally Berzins (n 83 above).

rights of data subjects. It specifically sets out most of the obligations of responsible parties as rights of data subjects. Section 5, thus, makes a wide range of obligations, such as notification, access, and correction rights of data subjects. It is submitted that there is no better way to advance the rights of data subjects in a data privacy law than the approach of the POPIA. Nevertheless, the POPIA does not contain the right to data portability which is an internet-specific right of contemporary relevance.[185] In this researcher's view, this goes to a broader issue of the debate on technology-neutral and technology-specific law which will be discussed subsequently. What is important at this point is a consideration of whether individuals have roles to play in the rights-based data privacy regime.

6.5.4. 'Reasonable' obligation of data subjects

Although it has been argued several times that safeguarding data privacy is largely the duty of government and business entities, the question remains as to whether an individual also has an obligation to protect his/her own personal information. This is more so in this era of what Allen refers to as 'great privacy give-away' whereby '[p]eople are giving away more and more personal data to intimates and strangers for a variety of self-interested, altruistic, or civic minded reasons.'[186] This 'era of revelation' is particularly problematic owing to the presence of the internet and social networking services (SNSs). Allen argues that, ordinarily, it is reasonable and prudent that a person is obliged to protect his/her data privacy.[187] She, however, particularly questions whether an individual has a moral/ethical obligation to protect his/her own personal information and whether such an obligation ought to be influenced by law.[188] This is because an ethical duty to protect one's personal information places 'more than merely prudential grounds for privacy vigilance.'[189] Although individuals' data privacy is entitled to rights protection based on the rights-based approach, individuals arguably have an ethical duty toward their own personal

185 Although subject to much debate. See P Bernal 'The EU, the US and right to be forgotten' in S Gutwirth *et al* (eds) *Reloading data protection law* (2014) 61-77.

186 A Allen 'An ethical duty to protect one's own information privacy?' (2013) 64(4) *Alabama Law Review* 847.

187 Allen (n 186 above) 850.

188 Allen (n 186 above) 850, the legal issues in merging law and ethic has been raise and discussed in GG Fuster & S Gutwirth 'Ethics, law and privacy: Disentangling law from ethics in privacy discourse' proceedings of the 2014 IEEE International Symposium on ethics in science, technology and engineering, 23-24 May 2014, Chicago. Available at http://works.bepress.com/cgi/viewcontent.cgi?article=1161&context=serge_gutwirth (accessed 1 November 2015).

189 Allen (n 186 above) 850.

information. Thus, after reviewing the views of various moral philosophers, Allen contends that:

> [i]n my view, people do indeed have a moral or ethical obligation to protect their own privacy (the same way they have a moral or ethical obligation not to lie, cheat, or steal) where privacy is understood as conditions of partial or complete observational and informational inaccessibility to others. Informational privacy requires limits on disclosure, limits on access, and data security. Favouring privacy over publicity is not a matter of taste alone, like the choice between a white or blue breath mint. On the contrary, there will be situations in which it can be morally imperative to choose privacy and obligatory not to forgo privacy.[190]

From the forgoing, a data subject is reasonably expected to protect his/her personal information. When a data controller, thus, has 'substantially' complied with the FIPs, it is only fair that reduced liability applies for risks resulting from a data subject's failure or gross negligence to observe ethical codes on the reasonable expectation with regard to the handling of his/her personal information.[191] This is consistent with the main essence of data privacy law which is not altogether to prohibit data processing as contended by De Hert and Gutwirth.[192]A rights-based data privacy regime merely ensures the fair and lawful processing of personal information based on dignity and the autonomy of the data subject.

The point must be stressed that the fact that some moral/ethical duty is placed on the data subject with regard to his/her personal information does not in any way diminish the obligation on the government (or data controllers generally) toward data privacy protection. Similarly, it does not place an impossible obligation on the data subjects. Responsibility in this case is for a fair and reasonable expectation of a data subject only. It is important to reproduce Allen's view on these issues *seriatim.* She states that:

> [t]oward concluding, I should emphasize my intention to avoid two implications: the implication that people have a duty to do the impossible and the implication that personal responsibility for one's own privacy precludes government and corporate responsibility for privacy protection. There are practical limits to how much people can do to protect their own privacy. Many of us are not sophisticated about the use of electronic technologies or the data gathering practices that are now commonplace. Some of us cannot avoid cultural and economic pressures to engage in transactions that result in

190 Allen (n 186 above) 863.

191 Even though I have argued in the previous chapter that liability in data protection law is strict. This is why Allen's proposal is merely an ethical or moral duty.

192 De Hert & Gutwirth (n 18 above) 3 where they contend that 'data protection does not have a prohibitive nature like criminal law.' Bernal view may seem to be at odds with the view of De Hert & Gutwirth in this regard because he contends that the default should be that data should not be collected. Bernal 2014 (n 1 above) 288.

> information disclosures. As individuals we have limited ability to negotiate with cloud service providers, internet browser providers, telecommunications carriers, app developers, and the government over privacy-related "terms and conditions." Protecting our information privacy is hard. But we are not completely helpless. We can disclose less or differently. That said, nothing I am arguing here should be interpreted as letting Big Data or government or others off the hook. As I stated in my introduction, I am suggesting a new, richer way to think about the moral relationship of consumers to business and government-as partnerships in ethical goodness.[193]

For individuals to be able to appreciate the risks that sometimes come with the processing of their personal information, the rights-based thesis advanced herein presupposes additional responsibilities on the government through the DPAs. Individuals must be properly educated and sensitised on their roles and obligations with regard to their personal information. I shall return to this point shortly.

6.5.5. Consent and rights-based approach to data privacy

Consent is indeed paramount in data privacy law; that is why it is specifically set out here and considered in more detail. Several data privacy scholars have emphatically stressed the importance of consent in data privacy law.[194] For example, Blume refers to consent as 'the most powerful tool of a data subject'.[195] Similarly, Bernal notes that consent is one of the keys to data protection; if you can obtain express, informed consent from someone to use their data, some of the key aspects of data protection law are effectively bypassed.'[196] On her part, Austin sees consent as 'the central vehicle in which … [data privacy] is accomplished.'[197]

---

193 Allen (n 186 above) 865.

194 Not only scholars, but also basic international instruments. Eg, the EU Charter expressly mentions consent as one of the legitimizing criteria for the processing of personal information in art 8. In providing for the right to data protection, art 8(2) requires that '[s]uch data must be processed fairly for specified purposes and on the basis of *the consent* of the person concerned or some other legitimate basis laid down by law.' [Emphasis added]. Albers, discussing the EU and German data protection regimes, observes that the right to informational self-determination protects the right to decide if one's personal information should be collected or used so as to prevent encroachment. It, therefore, means from such scope of protection, every step in the processing of one's personal data is considered as an encroachment on the right to informational self-determination. '[t]herefore, every step in *processing data must be based either on consent or* – more important – on constitutional legal basis which has to meet the requirements of the principles of clarity and determinedness and of proportionality.' [Emphasis added]. Albers (n 10 above) 220.

195 P Blume 'The myths pertaining to the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 270.

196 Bernal 2010 (n 1 above) 123.

197 L Austin 'Is consent the foundation of fair information practices? Canada's experience under the PIPEDA' (2006) 56 *University of Toronto Law Journal* 181. Even though she later 'call[s] into question the claimed centrality of consent to fair information practices and the data protection regimes

With regard to the thesis of a rights-based data privacy regime, consent is crucial as it fosters the human right to autonomy aspect of data privacy law. In other words, consent is the basis for individuals to express their choice and exercise control over their personal information. Brownsword rightly points out that 'taking [the] individual seriously, taking rights seriously, means taking consents and refusals seriously.'[198] In another work, Brownsword was more emphatic that '[i]n a community of rights, the principal (but not exclusive) function of consent is to authorise an act that would otherwise constitute a violation of a right.'[199] Although consent is not the only legitimizing factor for the processing of personal information, it is the basic means by which fair and lawful processing can be actualised.[200] It is, therefore, submitted that the requirement of consent is arguably half of data privacy law. Yet, 'the need for consent of a data subject can be derogated from'.[201] Austin was quick to mention that 'all derogations from consent are not necessarily derogations from privacy.'[202]

From the forgoing, it is submitted that a rights-based data privacy regime must acknowledge the pivotal role of consent and put mechanisms in place for its actualisation.[203] In this regard, a data privacy instrument must provide for express (explicit or unambiguous, 'opt-in') consent as against implicit (or deemed 'opt-out') consent.[204] An important characteristic of this kind of consent (explicit) which goes in line with the rights-based thesis is that 'mere inaction – just staying silent – must not be interpreted as

---

modelled upon them.' 182. See also De Hert and Papakonstantinou (n 28 above)135. Similarly, Brownsword emphatically stressed the centrality of consent in R Brownsword 'Consent in data protection law: Privacy, fair processing and Confidentiality' in S Gutwirth *et al* (eds) *Reinventing data protection?* (2009) 87.

198 R Brownsword *Rights, regulation and the technology evolution* (2008) 72. See also Kosta (n 19 above) 133.

199 Bronsword (n 197 above) 88.

200 Several other legitimizing factors for data processing are provided in data privacy law. The most controversial, apart from consent, is the requirement that data processing is justified for the purposes of pursing the legitimate interest of the data controller (responsible party). This is provided for in sec 11(f) of the POPIA. Similar effects of this justification are also present in sec 5(3) of the PIPEDA. Art 6(1) of the draft EU Regulation contains this legitimizing criterion which has been severely criticised. Hornung argues that it 'could potentially render the rest of Article 6 meaningless for private controllers, depending on which grounds are considered legitimate in this respect.' See G Hornung Abstract of the presentation for the Interparliamentary Committee Meeting titled 'The reform of the EU Data Protection framework – Building trust in a digital and global world'. Session II – Harmonised and strengthened data protection rights and principles for an interconnected world, 9/10 October 2012, Brussels available http://www.europarl.europa.eu/document/activities/cont/201210/20121008ATT53088/20121008ATT53088EN.pdf (accessed 1 November 2015).

201 Kosta (n 19 above) 137.

202 In her discussion on consent under the Canadian PIPEDA. See Austin (n 173 above) 183.

203 Kosta (n 19 above) 139.

204 See DJ Solove 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 53 *Stanford Law Review* 1458 for more discussions on 'opt-in' and 'opt-out' consent.

consenting.'[205] There must be a positive action for there to be consent.[206] This suggestion is without prejudice to the processing of personal information for law enforcement and other public purposes which must be narrowly construed.

Both the Canadian and South African data privacy regimes have arguably given consent its proper place in the overall scheme of data privacy protection.[207] In the Canadian Privacy Act, consent is a legitimate ground for data processing based on several provisions.[208] The kind of consent is, however, not specified. The PIPEDA, on the other hand, takes consent very seriously and, as a consequence, it is made an independent principle.[209] The PIPEDA, like the Privacy Act, does not also provide for this kind of consent. It is, however, arguable that explicit (informed) consent is envisaged since that Act makes reference to 'knowledge and consent' in several cases.[210] This may not, however, be the case as it is expressly provided that '[t]he form of consent sought by the organization may vary, depending upon the circumstances and type of information.'[211] Implicit and explicit consent are, thus, envisaged depending on the degree of sensitivity of the information. The Act, however, introduces a confusing criterion that 'any information can be sensitive depending on the context.'[212] The exact position of the PIPEDA with regard type of consent is, thus, still largely uncertain. Unlike the PIPEDA, the South African POPIA unequivocally requires consent to be explicit when it provides that 'consent means any *voluntary*, *specific*, *informed* expression of will in terms of which permission is given for the processing of personal information.'[213] The POPIA follows the draft EU Regulation in this regard.[214]

---

205 Kotschy (n 135 above).278.

206 This was based on an analysis of the Art 29 WP. See Kotschy (n 135 above) 278.

207 Eg, consent is a main justifying ground for all kind of data processing under the POPIA. It was mention 30 times in the Act.

208 Privacy Act, secs 7 & 8(1).

209 PIPEDA, clause 4.3 schedule 1.

210 Eg, clause 4.3.2 stipulates that 'the principle requires "knowledge and consent" Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.'

211 PIPEDA, clause 4.3.4.

212 PIPEDA, clause 4.3.4. However, it is still further provided in clause 4.3.6 that '[t]he way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).'

213 POPIA, sec 1.

214 See draft EU Regulation, art 4(8). See also De Hert & Papakonstantinou (n 28 above) 135.

Despite the mechanism for eliciting proper consent, actualizing it has proved to be extremely problematic in practice. This is more so the case with the current ubiquitous data processing environment characterised by the internet and highly sophisticated technological devices. Kosta was apt in her description of the problems of consent in contemporary internet-based society. She stated that:

> [r]ecent technological developments have introduced automatic processing of personal data and are challenging the functioning of consent as an act protective of the autonomy of the individual. When the consent can be expressed by the ticking of a box, there are no safeguards that the data subject has actually read the information that is provided before consenting and there is heated debate as to how consent can be provided in online environments… At the same time, in an online environment, the focus on the "communicative transactions by which consent is sought [and] given is extremely difficult, exactly because the communication between the agents is not direct anymore and has been substituted by standardised documents and online forms.[215]

Koops also describes this problem as the 'mythology of consent' and contends that 'consent is largely theoretical and has no practical meaning' as 'it is generally recognised that with internet-based services, most people just tick consent boxes without reading or understanding privacy statements, or that service providers sometimes assume that website visitors are somehow miraculously informed of the privacy statement and automatically give consent by merely visiting the website.'[216] Similarly, Bernal notes that '[c]onsent is a more complex issue than it seems – it is not simply a matter of getting user's consent before doing something.'[217]

The argument above has made some scholars seek alternatives to the consent requirement. For example, Kotschy argues that, because data subjects are not willing to invest time in checking information and the implications of consent clauses especially online and many data subjects are not in the position to evaluate the legitimacy and proportionality of the use of their data described in an information or consent clause, 'effective data protection should be sought on grounds other that explicit consent.'[218] She, therefore, argues that a

---

215 Kosta (n 19 above)138.

216 Koops (n 49 above) 252.

217 Bernal 2014 (n 1 above) 36. He further described the problem of consent especially with online services that '[o]n the internet, and indeed when dealing with computer software in general, the kind of consent generally gained is by a user scrolling down a long page of writing that they do not read and then clicking "OK" at the end to confirm that they have "read and understood" the terms and conditions. The information thus presented (but rarely read) is deemed to make the consent "informed", while the clicking of OK is deemed to make it "express".'

218 Kotschy (n 135 above) 280.

supervisory institution (DPAs and private institutions) will be a more effective institution to check the legitimacy of data processing rather than data subjects.[219] Prior authorisations, prior consultations and certification mechanisms or data protect seals should, thus, be employed.[220] Her suggestion is indeed very useful as a way of ensuring fair and lawful data processing. Its feasibility in this era of big data is, however, questionable. The continuous ubiquity of processing which is facilitated by technology means it will be increasingly difficult to identify data processors. While Kotschy's recommendation may be realistic in the case of big and known data controllers, it may be difficult to implement for other lesser controllers. Nevertheless, it must be said that her suggestion is very useful inasmuch as it does not totally sideline the requirement of 'explicit' consent.

Like Kotscky, Zanfir, in an article titled 'Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law', has also argued that more emphasis should be placed on 'stronger rights for data subject…and correlative obligations of the controllers and processors, which are applicable regardless of the legal basis for the data processing.'[221]

Other commentators are more radical in their recommendations for alternatives to consent. Austin, for example, argues 'that the alleged centrality of consent to the protection of privacy is misplaced'[222]. Thus, '[s]ome…other norms, such as the "reasonable purpose" standard included in the PIPEDA, can potentially offer a great deal of [data] privacy protection.'[223] Her argument was hinged on section 5(3) of the PIPEDA.[224] Reasonable purpose, according to this scholar, includes proper notification on purpose of data processing (collection, use and disclosure) and the requirement that a processing must be reasonable.[225] In other words, a controller may process personal information even without consent provided such processing is 'reasonable'. While not totally dismissing Austin's argument, it is submitted that it may not go down well with the rights-based thesis in this

---

219 Kotschy (n 135 above) 280.

220 She contends that '[t]he draft General Regulation foresees instruments for having such expert evaluation, partly by the data protection supervisory authorities in the course of prior authorization and prior consultation, and partly by private institutions entitled to apply certification mechanisms or data protection seals'. See draft EU Regulation, art 34 & EU Directive, art 39.

221 Zanfir (n 180 above) 238.

222 Austin (n 197 above) 183.

223 Austin (n 197 above) 183.

224 Reasonable purpose is based on sec 5(3) of the PIPEDA which provides that '[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.'

225 Austin (n 197 above) 183.

chapter for three reasons. Firstly, it totally removes the power of choice and control from individual and puts it on data controllers. In this case, an important question is where the autonomy of data subjects lies.[226] Secondly, her suggestion may be workable under employment contracts, as depicted in the article, but would hardly be so in other cases. This is because it may be argued that, by accepting employment, an individual is deemed to have consented to his/her data processing in certain cases, thus avoiding the need for express consent.[227] Similarly, it may be argued that such processing falls within other justifications for processing outside consent.[228] Thirdly, the suggestion of processing for 'reasonable purpose' as an alternative to consent may seem to be introducing unnecessarily vague criteria which may be an escape route for data controllers to avoid their obligations.[229] It is, therefore, submitted that this suggestion gives unnecessary concessions to business entities and is not suitable for a rights-based regime.

All the alternatives suggested above seem to be recommending greater enforcement and supervision of data privacy laws which is also in line with my thesis of a rights-based data privacy regime. Nevertheless, the point must be stressed that a rights-based regime, rather than looking for alternatives to consent, should seek to empower individuals to be able to give informed consent.[230] One such mechanism is the education roles of the DPAs. Also, consent must not be a one-off decision of either 'I agree' or 'I decline'. It must be a process.[231] This would be to enable a data subject to revoke consent at any time in the processing cycle.[232] Similarly, the drafting of data privacy laws in a proper form that is

---

226 Which, of course, is one of the philosophies behind data privacy law. Because of the complex nature of consent, Bernal asked the question '[d]oes that mean that the whole idea of consent should be abandoned?' To it, he answered that 'If autonomy is considered important, it cannot be. Instead, more radical solutions must be considered.' Bernal 2014 (n 1 above) 40.

227 Although I have argued earlier that deemed consent is not suitable for a rights-based approach.

228 Like legitimate interest of data subject etc.

229 They will simply argue that the collecting of their personal information is reasonable even when they know it is not reasonable. Moreover, it seems to be placing too much faith in the actions of data controllers which Koops has argued is not feasible. See Koops (n 49 above) 253.

230 Since one of the main arguments against consent requirement 'is that convenience and people's limited capacity to make rational decisions prevent people from seriously spending time and intellectual effort on reading the privacy statements of every website, app, or service they use.' See Koops (n 49 above) 252. This suggestion also seems to be similar to what Bernal has recommended that informed explicit consent should not merely entail giving information to make a decision but also to ensuring that such decision is understood. Bernal 2014 (n 1 above) 41

231 Consent being a process seems to be supported in the Canadian PIPEDA where it provided in clause 4.3.8 of the schedule that '[a]n individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.'

232 This suggestion is that of Bernal in his consideration of consent in the online world. He further recommends, based on an analogy of informed consent in medical law, that it should be an interactive process. Bernal (n 1 above) 41.

easily comprehensible is paramount in this regard. This view is without prejudice to stronger data privacy principles and enforcement which hold the data controllers strictly accountable for their data processing activities. Furthermore, these issues also invoke the ethical duties of a data subject towards his/her own personal information. We must, at least, make some effort to understand the terms and conditions of processing before we grant or refuse consent.

6.6. Data Protection Authorities (DPAs) as a vehicle for advancing a right-based approach to data privacy protection

Hustinx states that data privacy 'is special in the sense that it is considered to be in need of "structural support" through the establishment of an independent authority with adequate powers and resources.'[233] DPAs, obviously, play an important role for a serious government desirous of advancing a genuine individual-centred data privacy regime as they act as its representative on data privacy matters. They can act proactively and reactively to ensure compliance with FIPs. While not trying to underestimate the reactive measures available to the DPAs to elicit compliance with data privacy laws, it is the view of this researcher that the non-forcible proactive measure must be further explored. This will enhance a true rights-based data privacy regime.

DPAs have general powers to investigate and intervene and powers to engage in legal proceedings. Both the Canadian and South African DPAs have all these powers which are specially tailored to enhance the rights of data subjects.[234] With regard to their proactive powers, the Privacy Commissioner of Canada has powers to carry out audits and reviews of data privacy practices (in certain instances).[235] The South African POPIA is silent on the auditory roles of the Regulator. Such roles were, however, recommended by the SALRC.[236]

---

233 See P Hustinx 'The role of data protection authorities' in S Gutwirth *et al* (eds) *Reinventing data protection?* (2009) 133. He further pointed out that '[c]ertain other fundamental rights, such as the freedom of expression and the freedom of assembly and association, already have strong institutional stakeholders, such as the media, labour unions or political parties but that is not the case for data protection. Most of what is happening in this area is moreover invisible and often difficult to understand or deal with without technical expertise.'

234 See generally discussions in chapters 4 and 5 on the role of supervisory and oversight agencies in Canada and South Africa.

235 See discussion in chapter 4. See also Privacy Act, sec 37 & PIPEDA, sec 18 PIPEDA.

236 SALRC (n 41 above) para 7.2.191.

A very crucial proactive role of a DPA which is important for a rights-based thesis is the role of education. This role is crucial for African countries because it directly sensitises members of the public to their rights and the need for data privacy protection. Also, the low level of awareness of data privacy issues justifies the importance of this role.[237] Since the approach proposed here places greater emphasis on empowering the people to exercise their right to data privacy, this power is crucial. Indeed, Fialova has rightly observed that:

> [i]nformational self-determination encompasses a control over the individual's personal data. The control may be exercised by the individual if only he/she is aware of the rights and of the means to claim those rights. Without awareness of the right, this right becomes meaningless in practice. The control cannot be maintained in case of the individual's ignorance in relation to a particular legal instrument.[238]

Unlike the Canadian Privacy Act, the PIPEDA exhaustively provides for the educatory functions of the Privacy Commissioner.[239] The South African POPIA has more detailed provisions on the power to provide education of the Regulator which depicts its significance.[240] The power ranges from promoting an understanding of the provisions of the Act to undertaking programmes to promote the protection of data privacy.[241]

The above notwithstanding, a DPA must be ready to stand up to its responsibilities in terms of enforcement and ensuring compliance with the law. Adequate sanctions must be implemented against unlawful data privacy practice without fear and favour. This is why data privacy laws require that the DPA must be independent.[242] A rights-based approach envisages that they are not only theoretically independent but independent in practice. Although, the Canadian Privacy Commissioner does not have enforcement powers as the South African Information Regulator does, it is difficult to assess the impact of this on the rights of individuals. Nevertheless, DPAs play a crucial role in advancing an individual-centred data privacy regime.[243]

---

237 Makulilo (n 4 above) D. Jur thesis 36.

238 E Fialová 'Data portability and informational self-determination' (2014) 8(1) *Masaryk University Journal of Law and Technology* 47.

239 PIPEDA, sec 24. See discussions in chapter 4.

240 POPIA, sec 40. See discussions in chapter 5.

241 POPIA, sec 40. See discussions in chapter 5.

242 There is no such provision in any of the Canadian data privacy law discussed here. Independence, however, is a basic requirement provided under the South African POPIA, sec 39(b).

243 For indices of a very strong and efficient oversight and enforcement body see SALRC (n 41 above) 459.

6.7. Data privacy protection through non-legal mechanisms ('new-technologies'): Applying Lessig's theory

Legal scholars and policymakers are increasingly beginning to acknowledge the role of other non-legal mechanisms with regard to realising data privacy protection.[244] Lessig is one of the strongest voices in this regard with his seminal work which advocates the use of law, norms, market and 'code' (or architecture) to achieve effective privacy protection today. His theory, however, places great emphasis on code - design or architecture of a particular technology.[245] The reason for Lessig's theory is, arguably, that traditional legal instruments are unable to cope with modern day data processing challenges.[246] Since the rights-based approach proposed herein is meant to achieve a high-level data privacy protection, it is submitted that there is much to learn from the idea of 'proactively'[247] using technology to achieve data privacy protection.[248] Indeed, Clark cynically puts it that the 'answer to a machine is in the machine'.[249] A data privacy law that is rights-based should, therefore, support the regulation of data privacy by the use of technology. Nevertheless, the overall role of the law must be critical as Greenleaf points out that '[t]here is little convincing evidence over the last 40 years that any non-legal constraints (*without legislative backing*) can prove effective in protecting data privacy against business and government self-interest in expanded surveillance'.[250] Hornung makes a similar observation that '[w]ithout mandatory requirements *and legal incentives*, there is the risk that developers and controllers will not provide [privacy enhancing technologies] PETs to

---

244 Eg, market, morality and infrastructure. Greenleaf (n 5 above) 8. For more elaborate discussions on regulating technologies, see R Brownsword & K Yeung 'Regulating technologies: Tools, targets and thematics' in R Brownsword & K Yeung (eds) *Regulating technologies: Legal futures, regulatory frames and technological fixes* (2008) 3; R Brownsword 'So what does the world need now? Reflections on regulating technologies' in R Brownsword & K Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (2008) 23.

245 See discussions in chapter 2.

246 G Hornung 'Regulating privacy enhancing technologies: Seizing the opportunity of the future European data protection framework' (2013) 26(1-2) *The European Journal of Social Science Research* 182.

247 Indeed privacy by design (PbD) originated from the idea of privacy enhancing technologies (PET) and was developed by Ann Cavoukian. PbD is a paradigm shift from the traditional method of data privacy protection, which is essentially reactive, to a more proactive mode. See Cavoukian (n 154 above) 3. See also A Cavoukian 'Privacy by design' https://www.ipc.on.ca/images/resources/privacybydesign.pdf (accessed 1 November 2015) 4.

248 Using technologies also goes with the rights-based thesis in that above all, one of its foundational principles of the idea of PbD is that 'Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.' See Cavoukian (n 157 above) 29.

249 J Bing & T Dreiern *Charles Clark's: The answer to a machine is in the machine and other collected writings* (2005).

250 (Emphasis added). Greenleaf (n 5 above) 7. His view was based on a survey carried out by Bennett & Raab on most of the non-legal approaches which found 'little significant evidence of their success unless they are integrated into a data privacy regime.' 8.

their respective customers [data controllers].'[251] Therefore, '[b]y executing normative requirements as to the use of personal data, law and technology complement each other and form an "alliance" to protect personal rights.'[252] The question then is how such requirements should be integrated into the law.

Neither the Canadian nor South African data privacy regimes have direct provisions enabling the protection of data privacy by technologies, privacy enhancing technologies.[253] Indirect provision can, however, be read in the requirements for security safeguards in both the Canadian PIPEDA and the South African POPIA. In the PIPEDA, it is provided that personal information shall be protected by security safeguards which could include 'technological measures, for example, the use of passwords and encryption.'[254] Similarly, the POPIA provides that a responsible party must secure the integrity and confidentiality of personal information in his possession or under his control 'by taking appropriate, reasonable, technical and organizational measures'.[255] These provisions, however, have certain weaknesses. Firstly, they are not as forceful as they should be in enabling the protection of data privacy by the use of technology. Secondly, they are applicable only to information which is stored, and they are, arguably, not applicable to the collection process of such information. Thirdly, the provisions apply only to data controllers and not the developers of these technologies.[256] Even the draft EU Regulation has no direct provision enabling regulation by technology which makes it a basis of criticism in some quarters.[257]

---

251 Hornung (n 246 above) 181.

252 Hornung (n 246 above) 182. See also D. Klitou 'A Solution, but not a panacea for defending privacy: The challenges, criticisms and limitations of privacy by design' in B Preneel & D Ikonomou (eds) *Privacy technologies and policy* (2012) 92. The scholar contends that 'PBD solutions (and computer code) are not a substitute or replacement for law, but rather are complementary to law, and PBD is not an approach to replace lawmakers or lawyers with computer programmers or engineers. Computer code neither replaces lawmakers or lawyers. Moreover, computer code, when used to enforce privacy/data protection laws, is not or does not become law, but remains as the technical means for enforcing the laws.'

253 With regard to the Canadian PIPEDA, it was expressly stated that PbD was not specifically referred to. However, the Act and the courts encourage a flexible approach in application of data privacy principles. On this basis, PbD can be inferred. Cavoukian (n 157 above) 17.

254 PIPEDA, clause 4.7.3(c) schedule 1.

255 POPIA, sec 19(1).

256 Klitou noted that '[t]he existing legal provisions [in the EU] are also only applicable to data controllers/service providers, and primarily do not apply to technology manufacturers/developers. Moreover, the technical emphasis, found both in law and industry standards, is all too often focused on data security. As a result, there is a lack of guidance, binding rules and established industry standards on the technical solutions for ensuring the principles of privacy overall.' Thus '[w]hile data security is an important element of privacy protection, it is just one principle of privacy and not the whole picture.' Klitou (n 252 above) 88-89.

257 Hornung criticised the provision as being vague especially when compared to sec 3 of the Federal Data Protection Act of Germany. He further argues that the provision 'lacks any binding statement

Article 23(1) makes it an obligation for data controllers to implement relevant data privacy protection during the design process and when using a technology.[258] It provides that:

> Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

Hildebrandt and Tielemans observe that the provision targets only users of these technologies and not their designers or manufacturers.[259] In addition, it was contended that these provisions create a data protection obligation only and not necessarily a privacy obligation.[260] Similarly, Hornung criticises the provision as being vague especially when compared to section 3 of the Federal Data Protection Act of Germany.[261] He further contends that the provision 'lacks any binding statement concerning the design of the technology and does not mention general principles of data protection through technology at all.'[262]

Be that as it may, two factors are crucial for data privacy protection through technologies. Firstly, data privacy protection is supposed to be proactively considered at the planning stage of a particular technology and, possibly, made a mandatory requirement. Secondly, there should be two target groups of these regulations, viz. producers or manufacturers of these technologies and users (data controllers and data subjects).[263] It was, therefore, recommended that regulation by technology (privacy by design) should be directly incorporated into the principle of accountability thereby making the data processor obligated to put in place 'necessary mechanisms' to ensure that all the FIPs are complied with.[264] This seems to be in tandem with the concept of Privacy by Design (PbD) which is

---

concerning the design of the technology and does not mention general principles of data protection through technology at all.' Hornung (n 246 above) 186-187.

258 Draft EU Regulation.

259 M Hildebrandt & L Tielemans 'Data protection by design and technology neutral law' (2013) 29(5) *Computer Law and Security Review* 517. According to them, the idea is probably because 'they will force developers to come up with the right types of technologies.'

260 Hildebrandt & Tielemans (n 259 above) 517 a possible rationale for this, according to the authors, is because 'privacy is an open and essentially contested concept, and it would be very difficult to define which design actually protects privacy.'

261 Hornung (n 246 above) 186.

262 Hornung (n 246 above) 186-187.

263 Hornung (n 246 above) 183.

264 Hornung (n 246 above) 189. His views in this regard were based on a recent submission by the European data protection commissioner.

an idea 'of embedding privacy into the design specifications of various technologies', which is achieved by 'building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems.'[265] This is a better approach in that, even at the stage of collection of personal information, necessary measures will be put in place as a matter of responsibility. Embedding data privacy protection in the accountability principle does not, however, answer the question of how to make producers of these technologies bound under the law. It is submitted that making producers bound will be largely a duty of the enforcement institution (DPAs). Two ways in which DPAs can ensure compliance is through their proactive powers such as powers to conduct audits and privacy impact assessment and power to issue binding codes guiding manufacturers of technologies.[266]

6.7.1. Relevance of the debates on regulation by technology to Nigeria

An important question is: what relevance are debates on regulation of data privacy by technologies to Nigeria? Put another way, is a study into the use of technologies to enhance data privacy rights necessary in a country like Nigeria? Although Nigeria is not a large technology manufacturer as many developed countries are, these debates are important for a number of reasons. To begin with, Nigeria's large population on the internet[267] and other social networking services (SNSs) will mean its actions can hardly go unnoticed online. As a consequence, rules made by Nigeria could influence data controllers outside Nigeria and even manufacturers of technologies and software abroad. Similarly, within Nigeria, regulating the conduct of technology users and producers is not a theoretical or futile venture for a number of reasons.

Firstly, there are quite a number of internet service providers,[268] websites developers[269] and software producers[270] who can be obligated to render their services in a particular

---

265 Cavoukian (n 247 above).

266 Fortunately, the South African POPIA's approach in terms of powers of the Information Regulator to issue binding codes is insightful. This is not only due to exhaustive provisions but also because it is provided in sec 68 that 'failure to comply with a code of is deemed to be a breach of the conditions for lawful processing' and will be punished as such under chapter 10 of the POPIA.

267 The population of internet user has again increased recently. The Nigeria Communications Commission (NCC) puts the number of internet users at 88 million which is an increase from the population last year. O Kadir 'NCC puts number of internet users in Nigeria at 88 million' http://www.today.ng/archives/071365056-ncc-puts-number-of-internet-users-in-nigeria-at-88million/ (accessed 1 November 2015).

268 See 'Internet providers in Nigeria' http://www.satproviders.com/en/list-of-all-services/NIGERIA(accessed 1 November 2015). In fact, there is even an Association of Internet Service Providers in Nigeria -Internet Service Providers Association in Nigeria (ISPAN).

manner. With rules requiring technologies used in data processing to be compliant with the FIPs, data processing and databases of government agencies (like the Independent National Electoral Commission (INEC) and Nigeria Identity Management Commission (NIMC)) will have to guarantee data minimisation and anonymisation. This is so as to ensure that cases of security breaches have a minimal impact or no impact at all. Similarly, security agencies that install surveillance technologies and other security apparatus will have to impress on their manufacturers that the technologies must be designed in compliance with the FIPs. In addition, a data privacy regime with explicit rules on technology regulation will require banks and other institutions processing personal data to design their websites and software in a manner that ensures compliance with the rights of data subjects.

On another front, given the generally lax attitude towards data privacy protection and low level of awareness in Nigeria, enabling data privacy protection in the design of technologies will no doubt enhance data privacy protection in Nigeria. This is, however, without prejudice to the role of an effective supervisory agency.

6.7.2. Human rights-based arguments against regulation by technology

A number of human rights related debates surround regulation by technology.[271] The crucial question is the acceptability of these norm-creating and enforcing technologies *vis-à-vis* human rights and constitutional democracy. Most of these technologies that enforce human rights are usually created by private developers and, in many cases, they determine the set of rules to be infused in these technologies devoid of the normal process of legislative debates associated with the normal law-making process. Koops, therefore, questions the idea of technology enforcing or supplementing law as a regulatory instrument.[272] He contends that this idea raises democratic and constitutional issues.[273] This is because 'there are concerns that fundamental safeguards of democratic and constitutional values may not apply fully or perhaps at all to regulation by technology, while the impact on the behaviour of citizens can be as significant as the impact of legal

269 See eg, http://www.platgroupng.com/, http://biocence.co.uk/ .
270 See https://ng.linkedin.com/title/software-developer/nigeria (accessed 1 November 2015).
271 For a more elaborate consideration of some of these issues but specifically on PbD, see Klitou (n 252 above).
272 B Koops "Criteria for normative technology: The acceptability of 'code as law' in the light of democratic constitutional values' in R Brownsword & K Yeung (eds) *Regulating technologies: Legal futures, regulatory frames and technological fixes* (2008) 157.
273 Koops (n 272 above) 157.

norms enforced by legal procedures.'[274] Based on these concerns, Koops developed 'a systematic set of criteria for [the] acceptability of normative technology'.[275]After a review of extant literature, therefore, he suggests that the acceptability of normative technology should be based on primary and secondary criteria.[276] What is clear is that he does not reject the idea of regulation by technology but rather recommends that it should be infused by certain constitutional and democratic values.

A more direct argument against data privacy protection by technology is that raised by Lindsay and Ricketson.[277] These scholars are of the view that technology restriction limits personal autonomy. In their opinion, 'technologies may be designed in such a way as to either restrict the ability of users to make decisions about what they can do with the technology, or to maximise user choice.'[278] Yet, they admit that embedding behavioural rules within technology may over time promote social conformity.[279] In this researcher's view, the criteria developed by Koops above may also be applicable in this respect. Moreover, having a DPA play greater role over these technologies will go a long way to ensuring that the technologies are developed with due consideration of all current and future human rights concerns. This is why a very proactive DPA with a very strong research team is necessary for a regime of data privacy protection that is founded on human rights.[280]

6.7.3. Technology-neutral vs. technology-specific instruments/legislation

Related to the issue of the prominence of technology in a data privacy regime is whether laws should be couched in a technologically-specific or technologically-neutral manner.[281]

---

274 Koops (n 272 above) 160.

275 Koops (n 272 above) 167.

276 Koops (n 272 above) 168-169. The primary criteria includes human rights, other moral values, rule of law and democracy while secondary criteria includes transparency of rule-making, checking alternatives, accountability, expertise (independence), efficiency, choice (effectiveness), flexibility and transparency of rules.

277 Lindsay & Ricketson (n 26 above) 149.

278 Lindsay & Ricketson (n 26 above) 149

279 Lindsay & Ricketson (n 26 above) 149

280 Other arguments have also been raised against regulation by technology. Eg, see S Gutwirth *et al* "The trouble with technology regulation: Why Lessig's 'Optimal Mix' will not work" in R Brownsword & K Yeung (eds) *Regulating technologies: Legal futures, regulatory frames and technological fixes* (2008) 193. However, in my view, these arguments are hot human- rights-based.

281 A law that is technologically-specific will contain rules and terminologies that are directed towards a particular technology. Eg, it has been argued that the right to data portability and the right to be forgotten technology/internet-specific rules that is specifically targeted certain internet services such as SNSs and cloud services. Van der Sloot (n 25 above) 319; G Zanfir 'Tracing the right to be forgotten in the short history of data Protection law: The "new clothes" of an old right' in S Gutwirth *et al* (eds)

These debates also have an impact on the rights-based approach proposed in this chapter. Bernal observes that a technology-neutral law is close to a rights-based approach.[282] He noted that '[l]ooking from the perspective of individuals and their experiences rather than in detail at a particular form of technology gives more of a chance to set principles that can be applied when technology develop'.[283] He was, further, of the view that if the law is too technologically-specific, it can be sidestepped. Yet, if it is too general, it is hard to apply.[284] Hilderbrandt and Tielemans have, however, argued that 'to achieve a technology-neutral law, technology specific law is sometimes required' [285]as 'any type of legislation is in fact technologically specific, since our environment is always technologically mediated.'[286] They further stressed that 'though technology in itself is neither good nor bad, it is never neutral.'[287]

While not totally dismissing their arguments, making laws too technologically-specific may not be feasible for the realisation of the right to data privacy in African countries for a number of reasons. Firstly, laws generally do not keep pace with technological development in Africa. Thus, once laws are passed, they are hardly revised or reviewed even when it is obvious that they have outlived their usefulness. Related to that is the cumbersome process of passing new laws and the amendment of laws in African countries generally.[288]

Both the Canadian PIPEDA and the South African POPIA are generally technologically-neutral.[289] They do, however, contain certain technologically-specific provisions.[290] The

---

Reforming European data protection law (2015) 227. See also De Hert & Papakonstantinou (n 28 above) 137. On the other hand, a technology- neutral law is a law/rule that is not specifically directed at a particular technology but is rather coached in a broad manner so that it covers a wide range of issues and endures for a period of time.

282 Bernal 2014 (n 1 above) 224.

283 Bernal 2014 (n 1 above) 224.

284 Bernal 2014 (n 1 above) 224.

285 Hilderbrandt & Tielemans (n 259 above) 509.

286 Hilderbrandt & Tielemans (n 259 above) 509.

287 Hilderbrandt & Tielemans (n 259 above) 509.

288 The first Data Privacy Bill has been before the Nigerian legislature since 2008 without any progress. In the same vein South African POPIA took more than 10 years before the legislative house.

289 With regard the POPIA, the SALRC was of the view that 'any wording included in the legislation to deal with security measures must be technologically neutral.' Para 4.2.264. Furthermore, the SALRC recommended that 'rather than telling companies what specific security measures they must implement, the Bill requires companies to engage in an on-going and repetitive process that is designed to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented and ensure that they are continually updated in response to new developments. In most cases it does not require use of any specific security measures, instead leaving the decision up to the company. Key to the new legal standard is a requirement that security be responsive to the companies' fact specific risk assessment.' SALRC (n 41 above) 4.2.278.

Canadian Privacy Act was particularly targeted at personal information recorded in government databases- called personal information bank.[291] This legislation (Privacy Act) exposes some of the flaws of a technologically-specific law in that data processing has generally moved from the antiquated method of storing information in databases to storing information online and in clouds. As a result, new issues, which were not anticipated when the law was being drafted, have emerged. Hornung captures the problem of technologically-specify legislation in succinct terms when he notes that 'technologies should not constitute the general regulatory concept of data protection law as continuous technological change would either lead to the inadequacy of these regulations or to a never-ending process of amending the existent data protection laws.'[292]

One way to avoid the problem of technologically-specific vs. technologically-neutral design of data privacy law is by having a very proactive enforcement agency. This agency can supplement technologically-neutral legislation with other soft-laws such as the issuing of binding codes and guidelines. As new challenges come up, codes based on the FIPs should be established and such codes should be reviewed periodically. Indeed, the making of codes is a less cumbersome process than the amendment of laws. The South African POPIA's approach in this regard is very detailed and insightful.[293]

6.8. The rights-based approach and data privacy issues in Nigeria: Some reflections

This chapter has expanded the theory of a rights-based approach to data privacy protection, from mere founding data privacy on the right to privacy to stronger and individual-centred data privacy regimes. Accordingly, the point was made that the rights-based approach in the perspective considered in this chapter is designing a data privacy regime to give utmost priority, both theoretically and in practice, to the rights and interests of individuals. This part of the chapter briefly reflects on aspects of a rights-based approach that may be useful for Nigeria based on certain data privacy challenges identified in chapter three.[294]

---

290 Eg, POPIA, sec 69.

291 Numerous references were made to such banks in the Act. See sec 10 of the Act.

292 Hornung (n 242 above) 187. Even Hilderbrandt & Tielemans later observed that '[t]he point is not that legislation should always be technology-proof, but that technology specific legislation is only enacted if there is a necessity to address or to redress the impact of a technology on the substance of a legal right.' Hilderbrandt & Tielemans (n 259 above) 511.

293 See POPIA, secs 60-68 where elaborate provision is made on code of conducts.

294 Discussions here are very brief. More will be considered in the next chapter.

With regard to data processing activities by the government and its numerous agencies, there is no better way to hold them to their data privacy obligations than by stronger regimes on data privacy. This is comprised of a clear, detailed and well expressed rights and effective supervisory institution. Thus, the first issue to be considered is what the main concerns of individuals are with regard to processing activities of government departments. A consideration of these concerns is important because a rights-based approach must first 'look at issues from the perspective of the individual.'[295] The main concerns of individuals with regard to data processing activities by the government and its agencies[296] are those of accountability, security safeguards and use limitations. Because these agencies are statutorily required to collect personal information as part of their mandate,[297] other data privacy concerns are, arguably, not so obvious. A rights-based data privacy regime will ensure that these institutions are strictly held accountable for the personal information in their possession with increasingly detailed obligations toward such personal information.[298] The question in this regard is what the 'added value' of a rights-based approach is. The added-value is, firstly, that the rights of individuals are given uppermost consideration in the data processing activities of these institutions. These rights are protected with clearer rules with very few or no exceptions which are usually associated with government institutions. Secondly, since a rights-based approach envisages a data privacy regime deeply rooted in the Bill of Rights, these institutions will hardly be able to escape from constitutional obligations. With regard to surveillance practices by security agencies in Nigeria, a rights-based approach will ensure that data collection and surveillance must be strictly justified. Indeed, it has been pointed out that '[f]rom a "rights-based" perspective, the degree of surveillance should be strictly proportional to the ends sought to be achieved.'[299] Thus data privacy will be the default, and surveillance the exception.

---

295 Bernal 2014 (n 1 above) 232.

296 In this case, Nigeria Communication Commission (NCC); INEC and NIMC.

297 Eg, sec 5 of the Nigerian Identity Management Commission (NIMC) Act no 23 of 2007 provides that 'the commission shall create, manage, maintain and operate the National Identity Database, established under sec 14 of this Act including the harmonization and integration of existing identification databases in government agencies and integration of existing identification databases in government agencies and integrating them into the National Identity Database.' See also Nigerian Constitution, 3rd schedule part 1, sec 15(e) which provides that among the functions of the INEC is to 'carry out the registration of citizens of Nigeria into the National Identity Database.'

298 Including use of technologies like encryption, etc.

299 Lindsay & Ricketson (n 26 above) 147.

As regards the data processing activities of private entities in Nigeria, a genuine a rights-based approach will ensure that businesses recognise the supreme place of individuals and their interests. Businesses will be bound by detailed obligations towards individuals' personal information supported by well-expressed rights of individuals. Similarly, they will, in most cases, require explicit consent to process individuals' personal information. Stronger enforcement of data privacy laws with greater penalties for violation will see to effective data privacy protection. Moreover, well expressed obligations will ensure that business entities conduct their business in compliance with the law.

Finally, well expressed rights will ensure that Nigerians are aware of the rights towards their personal information. Furthermore, supervisory agencies will have a duty to ensure proper sensitisation of individuals with regard to risks associated with the processing of their personal information.

6.9. Chapter conclusion

This chapter has investigated how data privacy can be 'effectively' realised in the light of contemporary debates. It argued that one of the ways for the effective realisation of data privacy protection in any jurisdiction is to have a regime that is individual-centred, which was referred to as a 'rights-based regime' based on Bernal and a host of postulations of other scholars. Based on this hypothesis, it was contended that there is a disconnection between data privacy protection in theory and practice. While, superficially, data privacy regimes claim they are primarily individual-centred, the contrary seems to be the case. This is more so for African countries which, arguably, enact data privacy laws for purely economic purposes. The researcher has argued that this should not be the case because African, like Western countries are inhabited by human beings who are entitled to the protection of their personal information. In essence, a rights-based data privacy regime focussing primarily on data privacy protection frameworks needs to be tailored towards achieving a high-level of protection for the rights of individuals. Certain questions in the form of criticism of the conception of an 'individual-centred' data privacy regime were raised and an attempt was made to show why data privacy should indeed focus on the individual and his/her interests and rights to control the processing of his/her personal information.

The chapter further examined some contents of a data privacy law that can effectively promote the idea of a rights-based regime. Firstly, the researcher argued that, unlike what is done in some countries such as the USA, a data privacy law must have a substantial link with the Bill of Rights in a country for it to be truly 'rights-based'. This is because rights contained in the constitution enjoy constitutional protection. The approach of Canada and South Africa in this regard was reviewed, and it was found that South Africa is more in tune with the rights- based conception. Yet, the Canadian approach is also noteworthy by granting the primary data privacy laws a quasi-constitutional status.

With regard to the contents of data privacy legislation, discussions were divided into two broad groups. Some preliminary issues on data privacy and the proposal for a rights-based regime were considered first. I argued that a rights-based regime can be promoted even from the onset in the law-making process, the purpose/objective of the law, and the scope of the law. Furthermore, much focus was placed on the FIPs. Here, it was contended that there is need for increasingly detailed and specific obligations for data processors and more subjective rights for data controllers. The Canadian and South African approaches were compared with a view to determining which is in line with the thesis of a rights-based approach. Other issues, such as 'reasonable' obligations of data subjects towards their information and how consent requirement can be tailored towards the realisation of a high-level of data-privacy protection, were examined. It was also argued that, contrary to the general assumption, a high-level data privacy regime will not discourage the free flow of personal information.

The chapter also discussed the role of the oversight and enforcement institutions in realising data privacy protection. Here, much focus was placed on educative roles and other roles which are proactive in nature. Another issue that is the subject of current debates is the role of other non-legal mechanisms in realising an individual-centred data privacy regime. Emphasis was placed on new technologies. In addition, debates around whether a law should be technologically-specific or technologically-neutral were also considered.

In concluding, a brief attempt was made to show why a rights-based approach will be particularly well-suited for Nigeria based on a brief analysis of some of the major data privacy challenges in Nigeria. In essence, the approach proposed in this chapter is basically all about ensuring that data privacy laws and policies are primarily for the

purpose of protecting the individual's rights and not promoting economic or market interests. When the rights of individuals are promoted, business objectives will also be fostered. As was earlier observed, however, 'rights first and business later'.

The next chapter concludes this research by bringing together all the lessons learnt and recommending practical ways in which data privacy protection can be realised effectively in Nigeria.

Chapter seven

Summary, recommendations and conclusion

7.1. Summary

This study has basically investigated how data privacy can be protected effectively in Nigeria. The issue is topical in the wake of the rapid advances in Information and Communication Technology (ICT) in Nigeria and its desire to take human rights protection to the next level because of its maturing democracy. The study, therefore, proceeded from certain key assumptions based on the current data privacy literature. One such assumption is that data privacy is a fundamental human right which is beginning to distinguish itself as an independent human right.

Data privacy is the right of an individual to determine the destiny of his/her personal information since it is a significant aspect of the personality of such an individual. This *sui generis* right, as noted in chapter one, is increasingly under threat, especially in developing countries like Nigeria. This is because, while significant gains have been made in terms of ICT development in Nigeria, the legal system has always lagged behind in responding to continuing threats posed by these 'new technologies'. The problem is further compounded by the fact that Nigerian policymakers and the people are yet to appreciate some of these issues and how they constitute a challenge to human rights and fundamental freedoms. This is a reason why the researcher has devoted considerable space, in chapters one and two, to discussing the basic ambits of the right to data privacy and its significance in the current Nigerian information society.

In chapter one, it was pointed out that the right to protection of data privacy entails the legal protection of persons with regard to the processing of their personal information. It was also stated that personal information has, over time, become a valuable commodity, and it is increasingly sought by various entities for several purposes. The value of this personal information has now made its processing more prevalent today than ever before.

This is more so for a country like Nigeria which has only recently started appreciating the significance of personal information and the need for its processing. The general improvement in ICT in the country adds to this problem, as easier and quicker ways of exploiting this information are now being utilised. A number of concerns are associated with modern data processing, especially from the human rights perspective. Part of the concerns, as articulated in chapter one (1.1), include the impact of processing on key human rights, such as dignity, personality, autonomy and equality. It is from this premise that the researcher has argued for the necessity of data privacy to be taken seriously in Nigeria because of its human rights implications.

Based on the earlier assumption that data privacy, though a novel right, can arguably stand independently, the discussion in this thesis focuses on data privacy separate from privacy *per se*. This approach is motivated by the fact that studies that consider data privacy separately from privacy are generally lacking in Africa (in general) and Nigeria (in particular). Two theories identified in chapter one (1.6.1) show the *sui generis* nature of the right to data privacy. The separatist theory basically states that data privacy has an 'added-value' beyond the traditional right to privacy. The instrumentalist theory, which rejects the separatist theory, argues that data privacy, like privacy, is a human right with an intermediate value because it is basically for the realisation of other core values such as human dignity and personality. A combination of these two theories generally underpins the arguments made in this thesis, especially from the point of view of imperatives for legal reforms on data privacy in Nigeria.

Before the thesis delved into the state of data privacy in Nigeria, which is the focus of this study, a series of preliminary reflections on the rudiments of data privacy was carried out in chapter two. The discussion in this chapter was necessary for two reasons. Firstly, there was the need to show the scope of data privacy law so as to justify the arguments in subsequent chapters for the necessity of a right to data privacy in Nigeria. The second reason, which is connected to the first, is the need to show the emergence and development of data privacy which is also crucial for a proper understanding of what the contemporary human right is all about.

From the forgoing, the current significance of personal information was elaborately discussed in chapter two (2.2) where it was noted that personal information is now vital to private and public sector data users and individual data subjects. In the public sector,

personal information is necessary for the performance of core governmental functions such as research, planning, law enforcement and security purposes. While the state is a large data processor, it was observed in paragraph 2.2.2 of this thesis that the phenomenon of 'banalization of data processing' has recently been experienced. This is a general movement of data processing from the public to private sector and from large organisations to private persons. Indeed, the increasing commodification of personal information has made commercial entities desire this personal information increasingly. Unlike the public data processors, the private sector presents greater challenges because it is usually unregulated and interested only in their profit making drive. This creates a platform for massive data processing without due regard to the rights of individuals. A seldom considered significance of personal information is the significance for data subjects. In recent times we have seen data subjects trade their personal information on the internet for various products and services. It is because of the way individuals' trade their personal information that a school of thought argues in favour of property rights in personal information.

The contemporary value attached to personal information has created incentives for the invention of easy methods to facilitate its exploitation. The thesis considered some of these means, which include data processing by relatively traditional mechanisms like computers and databases to more complex and ubiquitous means such as the internet, clouds and surveillance technologies. Their profound effect on human rights was noted, and it was observed that the problem with these methods of data processing is that they becoming more invisible over time, which makes it difficult for individuals to know who holds what information about them. With time, therefore, concerted action was taken to curb the menaces resulting from data processing.

Initially, concrete action started at national level with a number of European and North American countries. Subsequently, data privacy became an international issue. International organisations, such as the Council of Europe (CoE), the Organisation for Economic Cooperation and Development (OECD) and the United Nations (UN), developed an interest in data privacy and adopted their respective data privacy instruments. The instruments of the first two organisations were, however, more influential than the UN instrument as was observed in paragraph 2.4.2. Nevertheless, all the instruments had a number of weaknesses identified in paragraph 2.4 such as ineffective harmonisation and a

weak enforcement mechanism. Because of the increasing need for harmonisation, regional institutions also took an interest in data privacy. Selected institutions in Europe, Asia and Africa were briefly considered. For Europe, it was stated that the EU has played the most significant role in the emergence and development of the *sui generis* right to data privacy. The current EU data privacy instruments (EU Charter and EU Directive) and the prospective instrument (the draft EU Regulation) are noteworthy. In Asia, the most notable instrument is the Asia-Pacific Economic Cooperation (APEC) Privacy Framework drafted by the APEC. Recent times have also witnessed the emergence of a number of African data privacy instruments such as the Economic Community of West African States (ECOWAS) Supplementary Act and the African Union (AU) Convention. These instruments are, however, not as influential as their European and Asian counterparts.

To provide a proper background to the essence of this study, an attempt was made to consider the debate on the commercial and human rights dimensions of data privacy. It was observed that, although the initial motivation for adopting data privacy laws was purely commercial, data privacy appears currently to have settled for human rights. How far African countries have been able to appreciate this fact is still uncertain, as shown in chapter six (6.2.2). Related to the issue of data privacy as a human right, is its exact relationship with the right to privacy. This thesis has admitted that, although it may be practically impossible to dissociate data privacy from privacy, data privacy has an 'added-value' especially in today's digital society. Data privacy, therefore, has a broader scope than the right to privacy in terms of the protection of personal information. It also promotes the personality rights of individuals and serves other interests of significance in the digital age. In spite of the unique nature of the right to data privacy, it was found that it is increasingly been considered to be an integral part of the right to privacy. A reason for this understanding is the extremely broad nature of the right to privacy. Right from Alan Westin's influential information control theory, therefore, data privacy is usually taken as a subcategory of the right to privacy in many jurisdictions such as Canada and South Africa. Scholars like Neethling also subscribe to Westin's theory on data privacy (called information privacy or data protection). It was, however, submitted that, irrespective of the nomenclature, a regime that protects personal information which is not necessarily 'private' or 'secret' is a data privacy regime within the context of this thesis.

Based on the background laid in chapters one and two, which has unequivocally shown the significance of data privacy, chapter three examines the state of data privacy in Nigeria. An attempt was made to show why the country needs to take data privacy seriously. This was done by examining where Nigerian society is currently in terms of ICT penetration and recent information processing activities which pose significant risks to individuals. With regard to ICT penetration, Nigeria has significantly improved in terms of internet and mobile telephone access and usage. This can be seen from the fact that Nigeria is the eighth largest user of the internet in the world. The large percentage of internet users is not merely a result of Nigeria's vast population but also an indication of the increasing digitalisation of the country. A number of data processing activities in the public and private sector were identified. It is based on these issues that chapter three (3.3) proceeded to evaluate the legal framework for data privacy in Nigeria. A number of key observations were made. Firstly, data privacy is currently protected by the Constitution, common law, legislation, soft laws, and regional instruments. Secondly, all these instruments provide little or no protection for data privacy based on the understanding of the term presented in chapter one (1.6.1). This is because they merely promote the secrecy or confidentiality of private information and do not, strictly speaking, grant individuals rights over their non-private information. The Nigerian courts have not been effective in data privacy issues largely because of a general lack of appreciation of the right to data privacy. People, thus, do not bring matters on data privacy violation before the court so as to present a platform for judicial activism which may be a catalyst to subsequent legislative reforms in this area.

Some efforts have been made by the Nigerian legislature to enact a data privacy law. These initiatives, however, arguably lack the requisite political will to be pushed through. One reason for the lack of political will is that data privacy is simply not taken as an issue of priority. Beside the absence of political will, a cursory look at the draft bills show that they may not achieve the desired level of data privacy required for Nigeria because of considerable flaws in their provisions. All in all, there is virtually little or no data privacy protection in Nigeria in spite of the growing level of the processing of personal information.

The above finding that data privacy is virtually unprotected in Nigeria, inspired the need to search for solutions. In this regard, Canada and South Africa were selected because of their, one hopes, sound legal regimes. The legal framework of data privacy in both

jurisdictions was examined in chapters four and five where a number of possible useful lessons were noted. Both jurisdictions have unique approaches to data privacy protection which may be useful for Nigeria from a comparative perspective. While South Africa adopts a comprehensive approach in line with the EU, Canada, arguably has a co-regulatory approach with substantial influence from both the US and the EU. The conceptual basis of data privacy in both countries also differs. While data privacy in Canada is for the purpose of the protection of the autonomy of Canadians, data privacy is for the protection of dignity in South Africa. The conceptual background of the South African data privacy regime is largely influenced by the concept of *Ubuntu,* which also underpins all rights in the Bill of Rights of the Constitution. The conceptual basis is not the only difference between the Canadian and South African data privacy regimes. Both countries also have quite dissimilar legal regimes for data privacy. The primary source of data privacy law in both countries is the Constitution. Unlike South Africa, however, Canada does not have a right to privacy included in its Bill of Rights. Data privacy (and privacy), thus, is basically read into the provisions of sections 7 and 8 of the Canadian Charter. South Africa, on the other hand, protects privacy in section 14 of its Constitution. As earlier noted, South African jurists and scholars have held that data privacy is an integral part of the right to privacy, and so it is protected under section 14. With regard to the statutory framework of data privacy, both countries also vary considerably. While Canada has multiple laws on data privacy at the federal and provincial level, South Africa has only one law. Another difference between both jurisdictions with regard to these laws is that Canada, unlike South Africa, regulates the private and public sector separately.

A brief overview of the data privacy legislation of both countries was undertaken. With regard to Canada, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA) were examined. The Protection of Personal Information Act (POPIA) was identified as the comprehensive data privacy law in South Africa. Even in these laws, a number of differences exist, apart from the scope identified earlier. While the Canadian Privacy Act, which regulates the public sector, does not explicitly provide for the Fair Information Practices (FIPs), the PIPEDA (for the private sector) provides for ten FIPs which are contained in the Schedule of the Act. The South African POPIA, on the other hand, provides for eight FIPs which are made an integral part of the law. Similarly, in the substance of the FIPs, considerable variation exists. For example, while the Canadian laws do not provide for a special regime for sensitive information, the South

African POPIA contains elaborate details relative to sensitive data processing in section 26. Both the Canadian and South African laws are also similar is some respects. For example, the laws of both jurisdictions were drafted by experts in the field of data privacy law. Similarly, the *travaux préparatoires* of the laws are detailed and serves as a useful resource for comparative legal researchers.

Both Canadian and South African data privacy regimes provide for an independent Data Protection Agency/Authority (DPA) which is to oversee the implementation of the various Acts. Considerable differences, however, exist in their nomenclature and structure. While the DPA is the Office of the Privacy Commissioner in Canada, the Information Regulator is the overall enforcement body of the South African data privacy legislation. Although both DPAs have similar policy instruments to ensure compliance with data privacy law, they vary in the powers they wield. The Canadian Privacy Commissioner, unlike the South African Information Regulator, does not have powers of enforcement. The Canadian Privacy Commissioner, unlike his South African counterpart, cannot directly enforce his/her decisions and recommendations. What this means is that in Canada the court is the institution to enforce data privacy law. This also shows a considerable difference between both regimes as the role of the South African courts in data privacy protection is not as extensive as that of the Canadian courts. In fact, the Canadian courts have the powers to reach a decision without paying attention to the findings of the Privacy Commissioner.

Based on an earlier assumption that a rights-based approach is useful for effective data privacy protection, the thesis, in chapter six, examined what the approach is all about. It was noted that the rights-based approach to data privacy is usually associated with the European approach (EU) to data privacy protection. The initial conception of the approach is that it is all about anchoring data privacy protection on fundamental rights and, in particular, the right to privacy. This thesis, however, expanded the scope of this approach based on the current literature. It was, thus, argued that the rights-based approach is not all about anchoring data privacy protection on fundamental rights but also about making the data privacy regime to be 'individual-centred'. This discussion is useful because African countries (in general) and Nigeria (in particular) seem mistakenly to see data privacy protection as being essentially for commercial purposes. This is thanks to the EU regime, especially its adequacy requirement in articles 25 and 26 of the EU Directive, where the perception is that data privacy laws are to be enacted so as to enhance Transborder Data

Flows (TBDF) at the expense of individual rights. Based on a comparative analysis of specific focus areas of the Canadian and South African data privacy regimes, a rights-based data privacy regime was proposed for Nigeria.

7.2. Recommendations

In the light of the various issues on data privacy protection raised in chapters one, two and three, and based on lessons obtained from the discussions in chapters four, five and six, the research recommends several measures as the way forward for the effective protection of data privacy in Nigeria. These measures are: the entrenchment of data privacy as a human right in the Constitution; the need for a 'rights-based' data privacy law; the involvement of other (human rights) institutions; the need for an active interaction with international data privacy regimes; the need to adopt regional and sub-regional data privacy instruments; the need for a proactive judicial system; the need to improve the level of awareness on data privacy and the need to boost scholarship and research on data privacy. These measures shall be discussed in detail.

7.2.1. The need for data privacy to be recognised as a human right and to be constitutionally entrenched

The first, and indeed most important way in which effective data privacy can be realised in Nigeria is that data privacy should be recognised as a human right. It has been stated in the previous chapters that, although data privacy has its commercial dimension, the human rights perspective appears to be dominating contemporary discourse on the subject. With all these debates and the fact that even key officials of the UN have recognised data privacy as a human right, the Nigerian government needs to approach data privacy from this standpoint. Furthermore, policymakers need to understand that, in terms of contemporary human rights, data privacy ranks among the highest. This is more so with the steady improvement in ICTs in Nigeria. Indeed, the Canadian and South African governments recognised the human rights implications of data privacy which is why they have taken specific actions with respect to it.

With policymakers recognizing and acknowledging data privacy as a human right, there will be sufficient incentives for it to be constitutionally entrenched. Constitutional entrenchment of the right is important because it will place a mandatory obligation on the Nigerian government to put in place all the necessary legal machinery to ensure its

actualisation. While it is admitted that a constitutional amendment is a very difficult process, it is recommended that future amendments should consider the prospects of establishing a right to data privacy. In this regard, the Nigerian legislature should take advantage of the on-going debate on constitutional amendment in Nigeria. Irrespective of whether data privacy is recognised as an independent right (as is the case in the EU and some European countries) or subsumed under the right to privacy (as in many other jurisdictions), data privacy must be constitutionally entrenched. The Constitutions of Cape Verde, Kenya and Mozambique, as earlier noted, are examples of African constitutions that explicitly provide for data privacy, albeit in a very restricted form (chapter six - 6.3). This shows, at least, that explicit constitutional recognition of data privacy is feasible in an African country. Another area that should be considered in future constitutional amendments is the removal of the discriminatory phrase in section 37 of the Nigerian Constitution which makes privacy protection applicable only to Nigerians.

Pending when the Nigerian legislature concludes discussions on the proposed constitutional amendment, the South African approach shows some insights useful for Nigeria. From the South African Constitutional Court's decision in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit,* jurists have inferred the right to information self-determination as was pointed out in chapter five. Nevertheless, the South African approach in this regard can be exercised only by a proactive and activist judiciary. The Canadian approach, on the other hand, may not be particularly useful for Nigeria because of the extremely narrow confines within which the Canadian Charter operates, as identified in chapter four. The fact that the Supreme Court of Canada has held that both the Privacy Act and the PIPEDA are quasi-constitutional statutes, however, shows the importance the country attaches to the protection of personal information.

7.2.2. The need for an explicit 'rights-based' data privacy law

All over the world, policymakers and scholars have acknowledged the significance of a comprehensive data privacy law in realising the right to data privacy. Indeed, the analysis of the Canadian and South African data privacy regimes in the previous chapters justifies this fact. Although there are a number of data privacy bills in Nigeria, it is recommended that they be discarded or substantially overhauled because of their significant flaws as enumerated in chapter three (3.7). With regard to a proposed data privacy law, this thesis

recommends that Nigeria should learn from the experiences of Canada and South Africa in two respects, *viz*: in the process of preparation of the law and in the contents of the law itself. Recommendations shall be made in this respect.

7.2.2.1. Process of preparation of the law

In the process of preparing the law, a number of key recommendations are noteworthy. Firstly, there is the need for policymakers to understand that preparing a data privacy law is not something that should be done in haste. Indeed, the process of preparation of the South African POPIA discussed in chapter five shows insights in this regard, although the POPIA took an unduly long time. The need for a careful consideration of a law is necessitated by the complex issues involved in data privacy law making; it should not merely be a 'cut and paste' of foreign data privacy legislation. Secondly, it is recommended that the task of preparation of the law be placed within an institution like the Nigerian Law Reform Commission (NLRC). This recommendation is also based on the South African experience where the South African Law Reforms Commission (SALRC) was responsible for the preparation of the POPIA. Even in Canada, the legislators were not the ones directly involved in the research and preparation of either the Privacy Act or the PIPEDA. This task was delegated to task forces and special committees created for such a purpose. In this regard, the NLRC, although virtually moribund, must be revived, as it is the proper institution to 'undertake progressive development and reform' of laws in Nigeria.

Thirdly, the officials of the NLRC must work with a committee of specialists in data privacy law. This is largely due to the in-depth research required in drafting the law. Such experts must comprise renowned academics in the field of data privacy law. Similar to the SALRC committee on privacy, the committee must devote sufficient time to a careful evaluation of data privacy laws in other jurisdictions. This is because of the necessity of a comparative study in data privacy policy formulation as acknowledged in chapter one (1.6.3). Fourthly, it is recommended that the process of the preparation of the law must include wide consultation with relevant stakeholders and the people. The processes leading up to the South African POPIA and the Canadian PIPEDA are noteworthy in this respect. Indeed, consultation will also have the effect of improving the level of awareness which is grossly lacking in Nigeria. Fifthly, wide consultation should also involve the publication

and wide circulation of the discussion papers. The discussion paper leading up to the POPIA is a crucial source of data privacy law in South Africa.

7.2.2.2. Contents of the law

In considering what should be contained in a proposed data privacy law, the thesis recommends that such a law must adopt a 'rights-based' approach in line with discussions in chapter six. It is further recommended that the government must expressly mandate the committee to pay due regard to the human rights of individuals. Other considerations must be secondary only. What this means is that, similar to the approach adopted by the SALRC, human rights must be carefully balanced with the other objectives of the government.

With regard to the preliminary provisions of the law, quite a number of issues must be taken into consideration. Firstly, the purpose/objective of the proposed law must clearly reflect its human rights agenda. Section 2 of the South African POPIA shows more insight in this regard than section 2 of the PIPEDA which appears to be skewed in favour of a commercial agenda. Secondly, with respect to the scope of the proposed Act, it is recommended that rather than having two different pieces of legislation for the private and public sectors as in Canada, the approach of the South Africa is preferable. It is less complicated and would be more feasible for Nigeria based on the arguments canvassed in chapter five (5.7). Another important recommendation with regard to the scope of the law is that personal information must be defined in as wide a manner as possible similar to that in the Canadian PIPEDA and the South African POPIA.

Thirdly, since the FIPs are fundamental in any data privacy law, sufficient space must be devoted to them in a proposed data privacy law in Nigeria. Indeed, the approach of the South African POPIA shows great insight from a rights-based perspective as the FIPs are not only made an integral part of the Act but are also rights of data subjects in terms of section 5 of the Act. Apart from being as explicit and exhaustive as possible, it is recommended that certain key FIPs must be contained in the proposed Act. They are the processing limitation, purpose specification, use limitation, security safeguard, openness, individual participation, information quality and the accountability principles. These are the basic FIPs provided in both the Canadian and South African data privacy laws as analysed in chapters four and five. All the listed FIPs also, arguably, satisfy the EU

Directive's adequacy requirement. While there is still considerable controversy regarding the special regulation (or otherwise) of sensitive information, it is recommended that any proposed legislation in Nigeria adopts the Canadian approach rather than the South Africa approach. In both Canadian data privacy laws, there is no special regime for the processing of sensitive personal information based on the assumption that otherwise non-sensitive information may be sensitive depending on the context of the processing. All personal information must, therefore, be protected equally. Unlike the case in Canada, it is recommended that a proposed law should provide special rules on TBDF as in section 72 of the South African POPIA. Such rules should, however, provide for a regime for the determination of 'adequacy'. To make the proposed law extra-territorially applicable, the Canadian approach to TBDF where the duty of accountability is imposed on the data controller should also adopted (see chapter four - 4.4.2.3 (g)). This is, however, in addition to the rules on TBDF like that in the South African POPIA.

In line with the rights-based thesis canvased in the chapter six, fewer exceptions should be provided for the FIPs, and, if an exception must be provided, it must be narrowly construed by the relevant enforcement agency. Furthermore, it is suggested that, based on the discussion in chapter six (6.7.3), it is preferable that a proposed data privacy law in Nigeria should be technologically-neutral. This is because of the cumbersome process of amending laws in the country.

Finally, the fact must be stressed that enacting comprehensive legislation is not enough for the realisation of the right to data privacy in Nigeria. There is also the need for effective monitoring and an oversight institution. This brings to the fore the role of a DPA.

7.2.3. The need for a dedicated and 'independent' data protection agency/authority (DPA)

As was observed in previous chapters, much of the effective realisation of data privacy has to do with the DPA. It is, therefore, suggested that a DPA must be established in Nigeria. In establishing the DPA, many useful lessons can be learnt from Canada and South Africa. Canada, however, provides more practical lessons than South Africa because the latter is yet to establish a DPA. Nonetheless, quite extensive provisions on the Information Regulator are contained in the South African POPIA. With regard to the structure and functions of a proposed DPA in Nigeria, certain recommendations are vital.

Firstly and most importantly, the proposed DPA must be independent. Independence in this regard requires that the DPA should be shielded from the control, interference or manipulation of both the government and private sector. It is only in this way that it can function effectively. Both the Canadian data privacy laws and the South African POPIA require the establishment of an independent DPA. Secondly, it is recommended that the proposed DPA must perform the seven (or eight) key interrelated roles identified in chapter four (4.5.1). The DPA must act as an educator, a policy adviser, an auditor, a consultant, an international ambassador, an ombudsman and an enforcer. With regard to the role of an enforcer, it was noted that considerable differences exist between the Canadian and South African approaches. While the Canadian Privacy Commissioner does not have enforcement powers, the South African Information Regulator wields such powers. In Nigeria, it is recommended that the South African approach should be adopted. This is because Nigerian courts are overwhelmed by a backlog of cases. The DPA can, therefore, relieve the courts in this regard by being the first contact point of an aggrieved data subject. Nonetheless, a proposed DPA must, to a larger extent, harness its power of persuasion and legal sanctions should only be used as a last resort. It is further recommended that, as in the South African POPIA in section 40, all the key roles of the DPA must be explicitly stated in the proposed data privacy legislation.

Thirdly, it is recommended that only competent and experienced persons should be appointed to the DPA. A legal background should ordinarily not be a requirement to head the office of the DPA. As is shown in section 41 of the South African POPIA, however, it is desirable. Fourthly, to ensure the effectiveness of a DPA, its role must be significantly decentralised. Decentralisation is paramount for Nigeria because of the country's size in terms of geographical scope and population. In this regard, Canada shows more insight for Nigeria than does South Africa. In Canada each province has an independent Privacy Commissioner. On the other hand, section 41 of the POPIA merely provides that the Regulator shall consist of a chairperson and four other Regulators. The Canadian approach may, however, put considerable strain on the government purse. It is, thus, recommended that the DPA should be established in at least the six geopolitical zones of Nigeria.

Lastly, the DPA should be bestowed with the responsibility of ensuring the effective sectoral application of data privacy principles. In this regard, a lesson can be drawn from

section 40(1)(f) of the POPIA where provision was made for the Regulator's role in establishing codes of conduct and guidelines.

While DPAs are vital for the realisation of data privacy rights, the wide range of tasks which is bestowed upon them has, over time, been criticised. It is, therefore, recommended that other institutions should assist the proposed DPA in the carrying out of its functions, albeit indirectly.

7.2.4. The crucial role of other (human rights) institutions in Nigeria

From the discussions in chapter four, it will be seen that other institutions beyond the DPA play important roles in data privacy issues in Canada. Although it may be difficult to implement the complex structure of Canada, it is suggested that two institutions should play active roles in data privacy issues in Nigeria. This is more so because of the long time needed to establish a DPA as has been shown in the case of South Africa. Firstly, the National Human Rights Commission (NHRC) should take up a 'watchdog' role of data privacy protection. 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. Its extended mandate 'to include vetting of legislation at all levels to ensure their compliance with human rights norms' also make its role crucial in this regard. Moreover, scholars recommend that future interaction between DPAs and national human rights institutions is sacrosanct for effective data privacy protection at national levels.

The second institution is Non-Governmental Organisations (NGOs). NGOs are indispensable when it comes to issues of promoting awareness and sensitisation on data privacy issues. This is because NGOs have, over time, helped in the advancement of human rights generally in Nigeria. Another aspect where NGOs can play important roles is in the area of data privacy litigation. NGOs can help institute actions on behalf of aggrieved data subjects in court or report matters to the DPA and follow-up on their handling. While there are a number of foreign privacy based NGOs, such as Privacy International, Electronic Privacy Information Center (EPIC) and Article 19, there is no local NGO in Nigeria. These entities have made significant contributions to data privacy law especially with their country-wide publications on privacy and data protection issues. But more needs to be done beyond mere publications especially because of the peculiar

nature of the Nigerian society. The NGOs should further assist the government in meeting its international and regional obligations on data privacy by setting up various monitoring mechanisms. The role of human rights activists, public defenders and civil society is also noteworthy in this respect. The Nigerian government will, therefore, need to establish a very cordial relationship with these entities so as to benefit from their expertise and create an atmosphere where the people will enjoy their human rights in the digital age.

7.2.5. The need for active interaction between the data privacy regime in Nigeria and international data privacy regimes

A proposed data privacy regime in Nigeria should operate in concert with international data privacy regimes. The regime should create a framework for active interaction with international data privacy regimes so that developments on the international scene can be reflected in Nigeria. The absence of this enabling framework is one of the profound deficiencies of the extant draft bills on data privacy in Nigeria. As shown in chapter 4 (4.6 and 4.7), Canada has an active interaction with the OECD and the APEC on data privacy matters. It has also participated in key dialogues in the CoE. Indeed, there are a number of benefits attached to this level of interaction, such as facilitating international compliance and aiding investigation and enforcement.

Unlike Canada, South Africa has established a framework for interaction with international data privacy regimes in the POPIA. As shown in chapter five (5.8), a conscious effort was made to ensure that the POPIA is in harmony with international standards. Besides, a number of provisions in the POPIA require the Regulator to monitor developments in the international scene constantly. The Regulator's role as an international ambassador is explicit in sections 40 and 44 of the POPIA. In line with the South African approach, a proposed data privacy law must contain elaborate provisions requiring the proposed DPA to monitor developments on the international scene. A proposed DPA must also advise the government with regard to the necessity of the adoption and implementation of an international data privacy agreement such as the CoE's Convention which is open for ratification by any country irrespective of its geographical location as noted in chapter two (2.4.2). Furthermore, a proposed DPA in Nigeria must participate in, or be represented in, international gatherings on data privacy such as the International Conference on Data Protection and Privacy Commissioners.

7.2.6. The need to adopt and implement regional and sub-regional data privacy instruments: Monist vs. dualist approaches

As was noted in chapter three (3.8), Nigeria belongs to two regional bodies with data privacy instruments. Both the AU and the ECOWAS have data privacy treaties which ought to influence effective data privacy protection in Nigeria. The AU Convention and the ECOWAS Supplementary Act, as has been observed, may, however, not influence effective data privacy protection. This is so because of Nigeria's dualist approach to international agreement. Section 12 of the Nigerian constitution provides that an international agreement can take effect only if it is ratified and domesticated in Nigeria. It is the view of this researcher that this is, indeed, a barrier to the development of the jurisprudence on data privacy. This thesis, therefore, recommends that there should be a reconsideration of the provisions of section 12 of the Nigeria Constitution. The South African approach in this regard seems good as it provides for a combination of dualist and monist approaches in section 231 of the South African Constitution. Based on section 231(3), an international agreement may be directly applicable if it does not require ratification or accession. It is, therefore, arguable that the ECOWAS Supplementary Act does not require ratification or accession so, if Nigeria's Constitution is amended to reflect the approach of South Africa, the Supplementary Act will be directly applicable.

Be it as it may, Nigeria should ratify the regional data privacy instruments that bind it, especially the recent AU Data Protection Convention. Ratification should not be a mere symbolic endorsement of these instruments, but, rather, Nigeria must also respect its obligations under these international treaties. The necessary mechanism must be put in place to actualise rights contained in the regional data privacy instruments. Further impetus in this regard can be fostered if a proposed data privacy law provides the necessary framework for interaction between a Nigerian data privacy regime and international regimes. Thus, Nigeria must take a leaf from provisions like section 44(c) and (d) of the South African POPIA which acknowledges the importance of international (and regional) treaties.

On the whole, there is an urgent need for Africa to develop data privacy at the continental level. In this regard, crucial lesson could be taken from the EU and APEC. Over time, regional data privacy instruments have proved to be the most successful and influential in

data privacy protection. Nigeria should lead the course for effective data privacy at continental level in the future because of its leading role on the continent.

7.2.7. The need for a proactive and 'activist' judicial system

Although judicial activism (judicial law making) is usually frowned upon as not being in line with democratic principles and values, data privacy law has largely developed through the 'activist' role of courts. As was earlier noted, in South Africa and Canada the courts have played a very significant role in constructing a constitutional right to data privacy even though such was not originally contained in the Constitution. In the light of the Canadian and South African experiences, it is suggested that judges in Nigeria must break from their 'shell of conservatism' and be more creative so as to enable the development of the jurisprudence on data privacy in Nigeria.

To make the judiciary more proactive in relation to data privacy issues, the thesis recommends the following. Firstly, there is the need for judges to be abreast of contemporary development in human rights. With respect to the right to data privacy, there is a need for the training and re-training of judges on the core values of data privacy. A better grasp of issues relating to data privacy will be reflected in their pronouncements and judgments and may ultimately be a catalyst for the recognition of independent data privacy rights in the near future. Regular training programmes should be organised with the collaboration of academics, a proposed DPA, and data privacy advocacy groups. Such training should also be a continuous activity. To make this suggestion more practicable, the Nigeria government could undertake to train particular judges for a start. They may also be encouraged to carry out postgraduate studies on data privacy law. Secondly, because of the general problems associated with litigation in Nigeria, it is suggested that the courts should play only an appellate role. Based on the Canadian approach, individuals may, thus, approach the court only as a last resort after they must have exhausted other resolution mechanisms, including the DPA.

Since judges do not engage in mere 'academic' or 'theoretical' exercises or act in a vacuum, the role of the people as prospective litigants comes to the limelight. This role cannot be exercised without an awareness on data privacy issues.

7.2.8. The need to improve the level of awareness on data privacy in Nigeria

An inference one can draw from the whole of the discussion in this thesis is that the awareness of the people (data subjects) is key to the effective realisation of the right to data privacy in Nigeria. As was noted in chapters one and three, awareness is grossly lacking in Nigeria. The problem is further complicated by the fact that people underestimate the risks involved in the processing of their personal information. The tricky question in this situation is how to achieve greater awareness with regard to the effective realisation of the right to data privacy in the country. In South Africa, awareness is higher because of the deeply entrenched protection of data privacy in the Constitution as well as the law of delict. Awareness is not an issue in Canada, as Canadian society is a developed Western society.

This thesis proffers three pragmatic recommendations as ways to improve the level of awareness in Nigeria. These recommendations are without prejudice to the little efforts individuals could personally make to be proactive with regard to their personal information by making the necessary complaint when infringements occur. Firstly, the proposed DPA must be very proactive in this regard. As was mentioned in the previous chapter six (6.6), the educational function is one of the key roles of the DPA. A DPA playing this role effectively is, thus, key to the realisation of the right to data privacy in Nigeria. Perhaps it is in the realisation of the importance of education that the South African POPIA makes an exhaustive provision in this regard. It is also made the first function of the Regulator in terms of section 40. The function includes organising programmes, public statements and giving advice. A similar provision is also contained in the section 24 of the Canadian PIPEDA. As was shown in chapter four (4.5.1), the Canadian Privacy Commissioner has, indeed, been playing this role very well. It is suggested that a proposed data privacy regime in Nigeria should adopt this approach. Similarly, the proposed DPA must learn from the Privacy Commissioner of Canada with respect to the performance of his/her role as an educator.

Secondly, the government, in collaboration with civil society groups, privacy advocates and academia should organise mass enlightenment and sensitisation programmes. Data privacy issues should also be widely publicised through all the major mass media services in Nigeria.

Thirdly, ICT law and human rights, with specific topics like data privacy, should be contained in the curriculum of universities at undergraduate and postgraduate level. This is because the subjects are, to the best of the researcher's knowledge, not contained in the syllabus of any Nigerian university. In South Africa, for example, ICT law is one of the modules taken by LL.B degree students. Furthermore, ICT law should be taken not only by law students but should also be taught, even if briefly, as part of the general studies courses offered by students in all Nigerian tertiary institutions. Such a module should also be taught from the African perspective by focusing on ICT issues in Nigeria.

7.2.9. The need to boost scholarship and level of research on data privacy in Nigeria

For the right to data privacy to be realised effectively in Nigeria, a crucial lesson learnt from Canada and South Africa is that the level of scholarship in Nigeria needs to be boosted. As stated in chapter one, scholarship on data privacy is very scanty in Nigeria. To the best of this researcher's knowledge, only three researchers have undertaken their doctoral and master's studies on data privacy in Nigeria. Similarly, there is little or no published scholarly work on the subject. For example, after extensive searches in renowned scholarly databases, the researcher could discover only about four (4) journal articles published on data privacy in Nigeria. This problem can be said largely to have been caused by three factors. Firstly, there is the issue of lack of awareness. Secondly, prospective researchers are simply not interested in the area because they perceive it as a largely theoretical issue. Thirdly, it is probable that because there is no data privacy legislation in Nigeria there is little interest in the subject.

In Canada, the level of data privacy scholarship is remarkable. Apart from a number of academics who have taken an interest in the subject, the regular publication from the Office of the Privacy Commissioner is also a very important source of knowledge as was noted in chapter four. Similarly, as was observed in chapters one and five, when it comes to the literature on data privacy in Africa, South Africa always takes the lead. This was so even before the passing of the POPIA. An improved scholarship level is important as it has the effect of enhancing the level of awareness on data privacy. It may also trigger the much-needed legal reforms in this area. Besides, a better scholarship level will enhance the expert network to facilitate Nigeria's participation in international and regional data privacy gatherings.

It is recommended that the government should create an enabling environment for the people to carry out more studies on the subject. Necessary funds and scholarships should be made available to willing researchers to undertake degrees and attend programmes (conferences, seminars and workshops) abroad. The Nigerian government should also collaborate with bodies like EPIC, Privacy International and International Association of Privacy Professionals (IAPP) to help in the training of people so that they are enabled to acquire the necessary skills in data privacy. Nigerian universities must also establish specific projects on data privacy with the support of the government. Academics should increasingly collaborate and carry out joint research projects with scholars in other jurisdictions such as Canada and South Africa. This will foster the much needed cross-fertilisation of ideas.

The importance of (postgraduate) research in the field of data privacy law cannot be overemphasised and, therefore, it is recommended that special attention should be given to it. Indeed, more postgraduate research will improve the pool of experts in Nigeria. Even data privacy laws seem to acknowledge the importance of expertise by requiring that only experts be appointed to the DPAs. For example, the South African POPIA, in section 41, requires, among other things, that only experts must be appointed to the office of the Information Regulator. Postgraduate studies on data privacy, especially at the masters and doctoral level, should, therefore, be encouraged and should be a continuous process. In this regard, it is recommended that prospective researchers may do well to update this thesis because of the constant state of flux in technological development. Other grey areas that may be considered are data privacy protection specifically on the internet, the impact of regional instruments on data privacy in Nigeria, and the sectoral application of data privacy law in critical sectors like the health sector in Nigeria.

7.3. Conclusion

In conclusion, this thesis comes full circle to the fact that advances in ICTs in Nigeria have a significant impact on human rights and fundamental freedoms. Guaranteeing human rights in the digital age, especially in developing countries like Nigeria, is, indeed, a huge challenge. This is because ICTs are gradually becoming deeply entrenched in society. ICT has permeated the fabric of human lives, and its presence is increasing felt in all the major sectors in the country. Policymakers and academics must, therefore, continue to pay more attention to the effects of ICTs on human rights. In this regard, Nigeria must seek

innovative approaches to tackling emerging human rights challenges resulting from the proliferation of ICT. In contributing to the debate on seeking innovative solutions to the challenges of proliferation of ICTs, this thesis posed the question, 'How can the protection of data privacy be realised effectively in Nigeria?' In answering the broad research question, five sub-questions were raised and answered. Based on the sub-questions, this thesis concludes as follows.

Firstly, international institutions with their data privacy instruments have been very influential in the emergence and development of the *sui generis* right to data privacy. Although the initial actions towards data privacy protection started at national level, the role played by international data privacy codes, such as the OECD Guidelines, the CoE Convention and the UN Guidelines, cannot be overemphasised. Regional instrument have also played a significant role. The most influential instruments are, however, those of the EU. It is from the EU and some countries in Europe that the notion of data privacy as an independent human right began. Nevertheless, the singular act of the EU Charter in providing for the right to data privacy which is separate from the right to privacy heightened the debates on the separateness of the *sui generis* right. This is why, when it comes to issues of data privacy, it is very difficult to ignore the EU. In essence, this thesis submits there is a trend of continuous 'disentangling' of the right to data privacy from the right to privacy.

Another conclusion reached with regard to the right to data privacy is that many countries, including Canada and South Africa, are reluctant to view data privacy separately from the right to privacy. This is largely because of the information control theory of privacy which underpins the conception of data privacy in these jurisdictions. Scholars have, however, shown that there may be a danger in this approach because courts may determine data privacy breaches only in cases where such breaches constitute the violation of privacy. If, therefore, any unlawful data processing is established, the matter may not be upheld by the court until it also amounts to a violation of privacy. Hence, privacy criteria are infused into data privacy infringements thereby restricting the scope of the latter. The thesis, however, concludes that, with explicit data privacy laws which define personal information broadly and cover both private and public information relating to individuals as well as containing all (or most) of the FIPs, the right to data privacy can be fostered. The onus, however, lies with enforcement institutions to take note of this *sui generis* nature of the right to data

privacy so as to ensure its actualisation. All things considered, the thesis concludes that a discussion on the development of the data privacy right is important for Nigeria because various international institutions have held that the right to data privacy is a right of all human beings irrespective of their nationality and residence. This is why there are calls for the UN to adopt an international instrument containing all the FIPs as noted in chapter two. In fact, the argument in international policymaking and academic circles is that the right to data privacy has crystallised into a norm of customary international law as pointed out in chapter one.

Secondly, this thesis concludes that, based on the notion of data privacy enunciated in chapter one of this thesis, the extant Nigerian legal framework does not provide effective data privacy for individuals. The Constitution is discriminatory in that it is applicable to Nigerians alone. It is also extremely limited since it appears to be applicable only to private information. The courts have also not been effective in advancing data privacy rights largely because cases on infringements are not brought before them. The common law, and other laws that provide partial protection, are also limited to protecting confidential information. With the recent data privacy bills, hope may be restored that the necessary legal reforms are finally on the way. But such hopes are dashed when a careful scrutiny is carried out on the bills. While there are quite a number of scholars and privacy advocates that have continued to advocate for the adoption of a data privacy law, they do so mostly for a different agenda. Rather than reflecting on how data processing affects human rights, scholars push for the law so as to satisfy the EU adequacy requirement to foster trade with developed countries (especially Europe). There is, therefore, the need for a re-orientation on the value of data privacy in Nigeria.

Thirdly, based on a careful evaluation of the legal regime for data privacy in Canada and South Africa, the thesis concludes that Nigeria can learn many useful lessons from their experiences. Although the researcher admits that the legal frameworks of these countries are not perfect, they show insight in several aspects. Based on an analysis of the constitutional and statutory protection of data privacy in Canada and South Africa, the thesis concludes that crucial insights that can be gained from both jurisdictions include, firstly, the constitutional approach to data privacy protection where, although both countries do not have an explicit constitutional provision on the data privacy right, the courts have been creative in establishing such rights or rights with similar effects.

Secondly, both countries have carefully considered comprehensive data privacy pieces of legislation, although with different scopes. Thirdly, while both countries have provisions establishing a DPA, South Africa is yet to establish such a body. Useful insight may, however, be obtained from the provisions on the DPA in the South African POPIA. Both countries also show insight into the approach of establishing a nexus with international data privacy regimes.

Fourthly, the question was posed regarding how data privacy protection can be realised using a rights-based approach. Both the South African and the Canadian data privacy regimes have aspects which may be considered 'rights-based'. The South African regime, however, shows much more insight with regard to the rights-based approach. This thesis concludes, based on the analysis of the approach in chapter six, that what is needed in Nigeria is a rights-based regime which is 'individual-centred' and gives due regard to the human rights and freedom of the people. This conclusion does not mean that consideration should not be given to enhancing TBDF; such should not be the case. There is the need for a careful balancing of the rights of the people *vis-à-vis* the interests of other entities in facilitating trade. It must be stressed, however, that the realisation of human rights in one of the indices of an effective democracy and, therefore, human rights must take priority.

On the whole, the thesis concludes that data privacy is indeed a human right the time for which has come. The government ought, therefore, to carry out the above recommended reforms so as to ensure that the right is realised in Nigeria.

List of instruments

National

Canada

Access to Information Act RS 1985 c A-1.

Access to Information and Protection of Privacy Act, Northwest Territories SNWT 1994 c 20.

Access to Personal Information and Protection of Privacy Act, Newfoundland and Labrador 2015 SNL2015 c A-1.2.

An Act to Amend the Personal Information Protection and Electronic Documents Act Bill C-12 2011.

An Act Respecting Access to Documents Held By Public Bodies and the Protection of Personal Information Quebec RSQ c A-21.

An Act to Amend the Personal Information Protection and Electronic Documents Act (Order-Making power) Bill C-475.

An Act Respecting the Protection of Personal Information in the Private Sector, Quebec, 1993 c P-39.1.

Anti-Terrorism Act (Bill C-51) 2015.

Canadian Constitution Act 1867 to 1982 30 & 31 Victoria, c 3 (UK).

Canadian Criminal Code RSC 1985 c V-46.

Canadian Human Rights Act RSC 1985 c H-6.

Canadian Standard Association (CSA) Model Code for the Protection of Personal Information 1996 reaffirmed 2001 available at http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00076.html (accessed 1 November 2011).

Digital Privacy Act (Bill S-4) 2015.

E-Health (Personal Health Information Access and Protection of Privacy) Act, British Columbia SBC. 2008 c 38.

Freedom of Information and Privacy Protection Act, Manitoba CCSM c F175.

Freedom of Information and Protection of Privacy Act, Nova Scotia c 5 of the Acts of 1993.

Freedom of Information and Protection of Privacy Act, Nunavut SNWT (Nu) 1994, c 20.

Freedom of Information and Protection of Privacy Act, Ontario RSO 1990 c F31.

Freedom of Information and Protection of Privacy Act, Prince Edward Island 2001 c F-15.01.

Freedom of Information and Protection of Privacy Act, c F-22.01 of the Statutes of Saskatchewan, 1990-91.

Health Information Protection Act, Saskatchewan SS 1999 c H-0.021.

(Historical) Safeguarding Canadians' Personal Information Act Bill C-12 2011.

Personal Health Information Act, Manitoba 1997 CCSM c P33.5.

Personal Health Information Act, Newfoundland and Labrador's SNL 2008 c P-7.01.

Personal Health Information Act, Nova Scotia SNS 2010 c 41.

Personal Health Information Privacy and Access Act, New Brunswick SNB 2009 c P-7.05.

Personal Health Information Protection Act, Ontario 2004 S.O 2004 c 3.

Personal Information Act, British Columbia (SBC 2003) c 63.

Personal Information Protection Act, Alberta Statute of Alberta, 2003 c P-6.5.

Personal Information Protection and Electronic Documents SC 2000 c 5.

Privacy Act RSC 1985 c P-21.

Right to Information and Protection of Privacy Act, New Brunswick SNB 2009 cR -10.6.

Treasury Board Directive on Privacy Impact Assessment http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308 (accessed 1 November 2015).

Cape Verde

The Constitution of Cape Verde (1992) with amendments in 1999.

Germany

Federal Data Protection Act (BDSG), 1978.

Ghana

Data Protection Act, 2012 Act 834.

Japan

Act on the Protection of Personal Information (APPI) Law No 57 of 2003.

Kenya

The Constitution of Kenya, 2010.

Mozambique

The Constitution of the Republic of Mozambique (2004) revised in 2007.

Netherlands

The Constitution of the Kingdom of Netherlands (2008).

Nigeria

African Charter on Human and Peoples' Rights (ACHPR) (Ratification and Enforcement) Act of 1983 formerly Cap 10 Laws of the Federation of Nigeria (LFN) 1990, now Cap A9 LFN 2004.

Central Bank of Nigeria (CBN) Act, 7 of 2007.

CBN Guidelines for Licensing, Operations and Regulation of Credit Bureaus in Nigeria 2008 available at http://www.cenbank.org/OUT/CIRCULARS/BSD/2008/GUIDELINE%20FOR%20LICENSING%20CREDIT%20BUREAU%20IN%20NIGERIA.PDF (accessed 1 November 2015).

Constitution of the Federal Republic of Nigeria 1999.

Consumer Protection Council Act C25 LFN 2004.

Computer Security and Critical Information Infrastructure Protection Bill 2005 SB 254.

Computer Security and Protection Agency Bill 2009 SB 336.

Computer Misuse Bill 2009 SB 346.

Cybercrimes (Prohibition, Prevention etc) Act 2015.

Cyber Security and Information Protection Agency Bill 2012.

Cyber Security and Data Protection Agency Bill 2008.

Data Protection Bill 2010 HB 476.

Economic and Financial Crimes Commission Act (Amendment) Bill 2004.

Electronic Fraud Prohibition Bill 2008 SB 185.

Freedom of Information Act (FOIA) 2011.

Money Lenders Act Cap 124 LFN 1958.

National Health Act 2014.

National Information Technology Development Agency Act (NITDA) 2007.

National Identity Management Commission Act A587 of 2007.

National Information Technology Development Agency (NITDA) Guidelines on Data Protection (2013) available at http://www.nitda.gov.ng/download/dataprotection.pdf (accessed 1 November 2015).

NCC (Registration of Telephone Subscribers) Regulations, 35 of 2011.

Nigeria Communications Act (NCA) 19 of 2003.

Nigerian Communications Commission (NCC) Draft Regulation for the Registration of All Users of Subscriber Identity Module (SIM) Cards in Nigeria http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=72&Itemid= (accessed 1 November 2015).

Nigerian Evidence Act 2011. Formerly Cap E 14 LFN 2004.

Nigerian Postal Service Act Cap N127 LFN 2004.

Independent National Electoral Commission (INEC) Guidelines for Permanent Voter Card Distribution (2014) available at http://www.inecnigeria.org/wp-content/uploads/2014/02/GUILDLINES-FOR-PVC-DISTRIBUTION-FOR-COMMISSION.pdf (accessed 1 November 2015).

Interpretation Act Cap 192, LFN 1990 now Cap I23 LFN 2004.

Personal Information Protection Bill 2012.

Privacy Bill 2009 HB 240.

Statistic Act 9 of 2007.

Telecommunications and Postal Offences Decree 1995 (Formally Decree No 13 of 1995 now Advance Fee Fraud and Other Related Offences Act 1995).

Wireless Telegraphy Act (1961) now no 31 of Laws of Nigeria 1998.

Portugal

Constitution of the Portuguese Republic 1976.

South Africa

Constitution of the Republic of South Africa of 1996.

Electronic Communications and Transactions Act (ECTA) 25 of 2002.

National Credit Act 34 of 2005.

Proclamation by the President of the Republic of South Africa No. R. 25, 2014 available at http://www.sabinetlaw.co.za/presidency/gazette-notice/37544-25 (accessed 1 November 2015).

Promotion of Access to Information Act (PAIA) 2 of 2000.

Protection of Personal Information Act 4 of 2013.

Switzerland

Federal Constitution of the Swiss Confederation of 1999.

United Kingdom

Data Protection Act of 1998.

United States

Cable Communications Policy Act of 1984.

Fair Credit Reporting Act of 1970.

Gramm-Leach - Bliley Act of 1999.

Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009.

Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001.

Video Privacy Protection Act of 1988.

International

African Union (AU)

African (Banjul) Charter on Human and Peoples' Rights 1981.

African Charter on the Rights and Welfare of the Child 1990.

African Union Convention on Cyber Security and Personal Data Protection 2014.

Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security of 2012.

Asia-Pacific Economic Cooperation (APEC)

APEC Privacy Framework 2005.

Council of Europe (CoE)

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Trans-border Data Flows 2001.

Council of Europe Committee of Ministers Resolution (96) 9 on Observer status for Canada with the Council of Europe http://www.coe.int/t/der/docs/CMRes969Canada_en.pdf (accessed 1 November 2015).

European Convention for the Protection of Human Rights and Fundamental Freedoms 4.XI. 1950.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data CETS No. 108 of 1981.

Resolution (73) 22 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in Private Sector (adopted 26 September 1973).

Resolution (74) 29 on the Protection of Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector(Adopted 24 September 1974).

Economic Community of West African States (ECOWAS)

Supplementary Act A/SA.1/01/10 on Personal Data Protection with ECOWAS 2010.

Treaty of the Economic Community of West Africa States (ECOWAS) No 14843 of 1985.

European Union (EU)

Charter of Fundamental Rights of the European Union 2000/C 364/01 of 2000.

Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data No L 281/31 of 1995.

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 the free movement of such data (General Data Protection Regulation) of 2012.

Commission Recommendation 81/679EEC relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (1981) OJ L246/31 available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31981H0679&from=EN (accessed 1 November 2015).

Draft Charter of Fundamental Rights of the European Union, CHARTE 4473/00 of 2000 http://www.europarl.europa.eu/charter/pdf/04473_en.pdf (1 November 2015).

Treaty on the Functioning of the European Union (TFEU) C 326/49 of 2012.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community 306/1 of 2007.

Organisation for Economic Cooperation and Development (OECD)

OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data of 1980.

Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013.

Southern African Development Community (SADC)

SADC Data Protection Model Law 2012.

United Nations (UN)

General Assembly Resolution A/RES/68/167 on the Right to Privacy in the Digital Age adopted on 18 December 2013.

General Assembly Resolution A/RES/69/166 on the Right to Privacy in the Digital Age adopted on 18 December 2014.

Guidelines for the Regulation of Computerized Personal Data Files A/RES/45/95 adopted by the UN General Assembly (GA) on 14 December 1990.

International Covenant on Civil and Political Rights of 1966.

Universal Declaration of Human Rights 1948.

List of cases

National

Canada

Alteen v Informix Corp (1998) 164 Nfld & PEIR 301.

B(A) v Canada (Minister of Citizenship and immigration) (2002) FCJ 610.

(Privacy Commissioner), Re 2000 CarswellNat 1756 (CA).

Canada (Information Commissioner) v Canada (Transportation Accident Investigation & Safety Board) (2006) FCA 157 (CCA).

Canada (Privacy Commissioner) v Canada (Labour Relations Board) (1996) 3 FC 609.

Dagg v Canada (Minister of Finance) (1997) 2 SCR 403.

Eastmond v Canadian Pacific Railway (2004) FC 852.

Englander v Telus Communications, Inc (2004) FCA 387.

Hunter v Southam, Inc (1984) 2 SCR 145.

Lavigne v Canada (Office of the Commissioner of Official Languages) (2002) 2 SCR 773.

Lawson v Accusearch Inc (2007) 4 FCR 314.

Montana Band of Indians v Canada (Minister of Indian and Northern Affairs) (1989) 1 FC 143.

Nunavut (Minister of the Environment) v WSCC, (2013) NUCJ 11.

R v Duarte (1990) 1 SCR 30.

R v Edwards (1996) 1 SCR 128.

R v Fearon (2014) SCC 77.

R v Jones (1986) 2 SCR 284.

R v M (MR) (1998) 3 SCR 393.

R v Morelli (2010) SCC 8.

R v Plant (1993) 3 SCR 287.

R v Wong (1990) 3 SCR 36.

Regina v Oakes (1986)1 SCR 103.

Rodgers v Calvert (2004) 2004 CanLII 22082 (Ontario SC).

State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada (2010) FC 736.

Germany

Population census decision, Judgment of 15 December 1983 *Bundesverfassungsgericht* decisions vol 65.

Nigeria

Aoko v Fabgemi (1961) 1 All NLR 400.

General Sani Abacha v Gani Fawahinmi (2000) FWLR 533.

South Africa

Bernstein and Others v Bester and Others NNO (1996) (2) SA 751 (CC).

H, WS v W, N (2013) (2) SA 530 (GSJ).

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd (2001) 1 SA 545 (CC).

*Mistry v Interim National and Dental Council of South Africa (*1998) (4) SA 1127 (CC).

NM v Smith 2007 5 SA 250 (CC).

S v Makwanyane (1995) 6 BCLR 665 (CC).

The Teddy Bear Clinic for Abused Children & Anor v Minister of Justice and Constitutional Development & Ors (2013) ZACC 35.

The Registrar of Financial Services Providers v Catsicadellis and Botha Enforcement Committee Case No 6 of 6 November 2012.

Thint (Pty) Ltd v National Director of Public Prosecutions & Ors: Jacob Gedleyihlekisa Zuma, Hully v National Director of Public Prosecutions & Ors (2008) ZACC 13 Case CCT 89/07.

*Tshabalala-Msimang & Anor v Makhanya (*2008) (6) SA 102 (W).

United Kingdom

Campbell v MGN (2004) UKHL 22.

Coco v AN Clark (Engineers) Ltd (1969) RPC 41.

Durant v Financial Services Authority (2003) EWHC Civ 1746.

Vidal-Hall & Ors v Google Inc (2014) EWHC 13 (QB).

WB v H Bauer Publishing Ltd (2002) EMLR 145.

United States

Katz v United States 389 US 347 (1967).

International

Court of Justice of the European Union & European Court of Justice

Bavarian Lager case, CASE T-194/04 Judgment of 8 November 2007.

European Commission v Bavarian Lager [2010] ECR I-6055.

Österreichischer Rundfunk and others [2003] ECR I-4989.

Productores de Música de España (Promusicae) v Telefónica de España [2008] ECR I-271.

Rotaru v Romonia (2000) RJD 2000-V, App. No 28341/95.

Case 131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos and Mario Costeja González* (2014) ECR I-000 (nyr).

Bibliography

Books and chapters in books

Ahn, MJ & McNutt, J 'If we build it will they come? An appreciation of the Microfoundations of E-Government' in Dolićanin, C; Kajan, E; Randjelović, D & Stojanovic, B (eds) (2015) Handbook *of research on democratic strategies and citizen-centered e-government service* IGI Global: US.

Akanbi, MM (2012) *Domestic commercial arbitration in Nigeria: Problems and challenges* Lambert Academic Publishing (LAP): Saarbrücken.

Albers, M 'Realizing the complexity of data protection' in Gutwirth, S; Leenes, R & de Hert, P (eds) (2014) *Reloading Data Protection: Multidisciplinary insights and contemporary challenges* Springer: Heidelberg.

Allot, A 'African Law' in Derrett, JDM (ed) (1968) *An Introduction to legal systems* Sweet & Maxwell: London.

Allotey, AKE (2014) 'Data protection and transborder data flows: Implication for Nigeria's integration into the global network economy' unpublished LLD thesis, University of South-Africa: South Africa also available at http://uir.unisa.ac.za/handle/10500/13903.

Bayley, RM & Bennett, CJ 'Privacy impact assessments in Canada' in Wright, D & De Hert, P (eds) (2012) *Privacy impact assessment* Springer: Heidelberg.

Bennett, CJ (1992) *Regulating privacy: Data protection and public policy in Europe and the United States* Cornell University Press: Ithaca.

Bennett, CJ 'What happens when you book an airline ticket? The collection and processing of passenger data post-9/11' in Zureik, E & Salter, MB (eds) (2005) *Global surveillance and policing: Borders, security, identity* Routledge: London.

Bennett, CJ & Bayley, RM 'Video surveillance and privacy protection law in Canada' in Nouwt, S; De Vries, BR & Prins, C (eds) (2005) *Reasonable expectations of privacy?* TMC Asser Press: Hague.

Bennett, CJ & Raab, C (2006) *The governance of privacy: policy instruments in global perspective* MIT Press: Cambridge.

Bennett, CJ; Parsons, C & Molnar, A 'Forgetting, non-forgetting and quasi-forgetting in social networking: Canadian Policy and corporate practice' in Gutwirth, S; Leenes, R & De Hert, P (eds) (2014) *Reloading Data Protection: Multidisciplinary insights and contemporary challenges* Springer: Heidelberg.

Bernal, PA (2011) 'Do deficiencies in data privacy threaten our autonomy and if so, can informational privacy rights meet this threat?' unpublished PhD thesis, London School of Economics and Political Science: London also available at http://etheses.lse.ac.uk/321/

Bernal, P (2014) *Internet privacy rights: Rights to protect autonomy* Cambridge University Press: Cambridge.

Bernal, P 'The EU, the US and right to be forgotten' in Gutwirth, S; Leenes, R & De Hert, P (eds) (2014) *Reloading Data Protection: Multidisciplinary insights and contemporary challenges* Springer: Heidelberg.

Bing, J & Dreiern, T (eds) (2005) *Charles Clark's: The answer to a machine is in the machine and other collected writings* Norwegian Research Center for Computers and Law: Oslo.

Brownsword, R 'Consent in data protection law: Privacy, fair processing and confidentiality' in Gutwirth, S; Poullet, Y; De Hert, P; De Terwange, C & Nouwt, S (eds) (2009) *Reinventing data protection?* Springer: Heidelberg.

Brownsword, R (2008) *Rights, regulation and the technology evolution* Oxford University Press: Oxford.

Brownsword, R 'So what does the world need now? Reflections on regulating technologies' in R Brownsword & K Yeung (eds) Brownsword, R & Yeung, K (eds) (2008) *Regulating technologies: Legal futures, regulatory frames and technological fixes* Bloomsbury Publishing: New York.

Brownsword, R & Yeung, K 'Regulating technologies: Tools, targets and thematics' in Brownsword, R & Yeung, K (eds) (2008) *Regulating technologies: Legal futures, regulatory frames and technological fixes* Bloomsbury Publishing: New York.

Burkert, H 'Privacy – data protection: A German/European perspective in Engel, C & Keller, KH (eds) (2000) *Governance of Global Networks in the Light of Differing Local Value* Nomos Verlagsgesellschaft: Baden-Baden.

Bygrave, LA (2002) *Data protection law: Approaching its rationale, logic and limits* MIT Press: Cambridge.

Bygrave, LA (2014) *Data privacy law: An international perspective* Oxford University Press, Oxford.

Bygrave, L 'International agreements to protect personal data' in Rule JB & Greenleaf, G (eds)(2008) *Global privacy protection: the first generation* Edward Elgar: Cheltenham.

Cate, FH 'The failure of fair information practice principles' in Win, JK (ed)(2006) *Consumer protection in the age of the information economy* Ashgate: Aldershot.

Cavoukian, A 'Privacy by Design: Leadership, methods, and results' in Gutwirth, S; Leenes, R; De Hert, P & Poullet, Y (eds) (2013) *European Data Protection: Coming of age* Springer: Heidelberg.

Charlesworth, A 'Understanding and managing legal issues in internet research' in Fielding, N; Lee, RM & Blank, B (eds) (2008) *The SAGE Handbook of online research methods* SAGE: Los Angeles.

Craig, T & Ludloff, ME (2011) *Privacy and big data* (2011) O'Reilly: Sebastopol.

Currie, I & De Waal, J (2005) *The Bill of Rights handbook* Juta & Company: Claremont.

Currie, I & De Waal, J (2013) *The Bill of Rights handbook* Juta & Company: Claremont.

De Hert, P & Gutwirth, S 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalization in action' in Gutwirth, S; Poullet, Y; De Hert, P; De Terwange, C & Nouwt, S (eds) (2009) *Reinventing data protection?* Springer: Heidelberg.

De Hert, P & Gutwirth, S 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in Claes, E; Duff, A & Gutwirth, S (eds) (2006) *Privacy and the criminal law* Intersentia: Oxford.

De Terwangne, C 'Is a global data protection regulatory model possible?' in Gutwirth, S; Poullet, Y; De Hert, P; De Terwange, C & Nouwt, S (eds) (2009) *Reinventing data protection?* Springer: Heidelberg.

Devenish, GE (1999) *Commentary on the South African Bill of Rights* Butterworths: Durban.

Doi, A (1990) *Sharia: The Islamic Law* Ikhsan: Ibadan (previously Ta Ha: London).

Elder, D 'Canada' in Kuschewsky, M (ed) (2012) *Data protection & privacy: Jurisdictional comparisons* Sweet & Maxwell: London.

Eruaga, O 'The first year of the freedom of information Act: has it been tested?' Azinge, E & Waziri, F (eds) (2012) *Freedom of information law & regulation in Nigeria* Nigerian Institute of Advanced Legal Studies: Lagos.

Ezejiofor, G 'Sources of Nigeria law' in Okonkwo, CO (ed) (1980) *Introduction to Nigerian law* Sweet & Maxwell: London.

Finn, R; Wright, D & Friedewald, M 'Seven types of privacy' in Gutwirth, S; Leenes R; De Hert, P & Poullet, Y (eds) (2013) *European data protection: coming of age* Springer: Heidelberg.

Flaherty, DH (1989) *Protecting privacy in surveillance societies* University of North Carolina Press: North Carolina.

Flaherty, DH & Canada Department of Justice (1981) *The origins and development of social insurance numbers in Canada* Department of Justice: Ottawa.

Fuster, GG (2014) *The emergence of personal data protection as a fundamental right of the EU* Springer: Heidelberg.

Garner, BA (ed) (2004) *Black's law dictionary* Thomson West: US.

Gondwe, M (2011) 'The protection of privacy in the workplace: A comparative study' unpublished PhD thesis, University of Stellenbosch, South Africa also available at http://scholar.sun.ac.za/bitstream/10019.1/17849/1/gondwe_protection_2011.pdf

Graziadei, M 'Comparative law as the study of transplants and receptions', in Reimann, M & Zimmermann, R (eds) (2006) *The Oxford handbook of comparative law* (2006) Oxford University Press: Oxford.

Greenleaf, G 'APEC's privacy framework sets a new low standard for Asia-Pacific' in Kenyon, AT & Richardson, M (eds) (2006) *New dimensions in privacy law: International and comparative perspectives* Cambridge University Press: Cambridge.

Greenleaf, G (2014) *Asian data privacy law: Trade and human rights perspective* Oxford University Press: Oxford.

Gutwirth, S; De Hert, P & De Sutter, L "The trouble with technology regulation: Why Lessig's 'Optimal Mix' will not work" in R Brownsword & K Yeung (eds) (2008) *Regulating technologies: Legal futures, regulatory frames and technological fixes* Bloomsbury Publishing: New York.

Gutwirth, S & Hilderbrandt, M 'Some caveats on profiling' in Gutwirth, S; Poullet, Y & De Hert, P (eds)(2010) *Data protection in a profiled world* Springer: Heidelberg.

Hughes, A (2014) *Human dignity and fundamental rights in South Africa and Ireland* Pretoria University Law Press, Pretoria.

Hustinx, P 'The role of data protection authorities' in Gutwirth *et al* (eds) *Reinventing data protection?* Gutwirth, S; Poullet, Y; De Hert, P; De Terwange, C & Nouwt, S (eds)(2009) *Reinventing data protection?* Springer: Heidelberg.

Hustinx, PJ '(Future) interaction between Data Protection Authorities and National Human Rights Institutions in the European Union' in Wouters, J & Meuwissen, K (eds) (2013) *National human rights institutions in Europe. Comparative, European and international perspective* Intersentia: Cambridge.

Hutchinson, T 'Doctrinal research: Researching the jury' in Watkins, D & Burton, M (eds) (2013) *Research methods in law* Routledge: London.

Kasneci, D (2008/2009) 'Data protection law: Recent developments' unpublished PhD thesis, *Università Delgi Studi Di Trieste*: Italy.

Klein, K (2012) *Canadian privacy: Data protection law and policy for the practitioner* International Association of Privacy Professionals: Partsmouth.

Klitou, D 'A Solution, but not a panacea for defending privacy: The challenges, criticisms and limitations of privacy by design' in Preneel, B & Ikonomou, D (eds) *Privacy technologies and policy* Springer: Heidelberg.

Kodilinye, G (1982) *Nigerian law of torts* Sweet & Maxwell: London.

Kong, J; Xiaoxi, F & Chow, KP 'Introduction to cloud computing and security issues' in Cheung, ASY & Weber, RH (eds) (2015) *Privacy and legal issues in cloud computing* Edward Elgar: Cheltenham.

Koops, B "Criteria for normative technology: The acceptability of 'code as law' in the light of democratic constitutional values' in R Brownsword & K Yeung (eds) (2008) *Regulating technologies: Legal futures, regulatory frames and technological fixes* Bloomsbury Publishing: New York.

Kosta, E (2013) Consent *in European data protection law* Martinus Nijhoff Publishers: Boston.

Kuner, C (2003) *European data privacy law and online business* Oxford University Press: Oxford.

Kuner, C (2007) *European data protection law: Corporate compliance and regulation* Oxford University Press: Oxford.

Kuner, C (2013) *Transborder data flow and data privacy law* Oxford University Press: Oxford.

Laosebikan, FO (2007) 'Privacy and technological development: A comparative analysis of South African and Nigerian Privacy and Data Protection Laws with particular reference to the protection of privacy and data in internet cafes and suggestions for appropriate Legislation in Nigeria' unpublished Ph.D. thesis, University of Kwazulu-Natal, South Africa.

Lessig, L (2006) *Code 2.0* Basic Book: New York.

Lindsay, D & Ricketson, S 'Copyright, privacy and digital rights management' in AT Kenyon & M Richardson (eds) (2006) *New dimensions in privacy law: International and comparative perspectives* Cambridge University Press: Cambridge.

Lloyd, IJ (2011) *Information technology law* Oxford University Press: Oxford.

Lloyd, IJ (2014) *Information technology law* Oxford University Press: Oxford.

London, RW (2013) 'Comparative data protection and security law: A critical evaluation of legal standards' unpublished LL.D thesis, University of South Africa, South Africa.

Lynskey, O 'From market-making tool to fundamental right: The role of the Court of Justice in data protection's identity crisis' in Gutwirth, S; Leenes, R; De Hert, P & Poullet, Y (eds) (2013) *European data protection: Coming of age* Springer: Heidelberg.

Makulilo, AB (2014) *Privacy and data protection in Africa* Scholars' Press: Germanny.

Makulilo, AB (2012) 'Protection of personal information in sub-Saharan Africa' published *Dr Jur* thesis, University of Bremen, Germany.

Mansell, R 'Human rights and equity in cyberspace' in Murray, A & Klang, M (eds) (2005) *Human rights in the digital age* Glasshouse Press: London.

McIsaac, B; Shields, R & Klien, K (2011) *The law of privacy in Canada* Carswell: Toronto.

McNairm, CHH & Scott, A (2010) *Privacy law in Canada* Butterworths: Ontario.

McWilliam, B 'Canada' in D Campbell (ed) (2013) *The internet: Laws and regulatory regimes* Juris Publishing: Huntington.

Morley, D (2015) *Understanding computers in a changing society* Cengage Learning: Stamford.

Morley, D & Parker, CS (2013) *Understanding computers: Today and tomorrow, comprehensive* Cengage Learning: Stamford.

Murphy, JT & Carmody, P (2015) *Africa's information revolution: Technical regimes and production networks in South Africa and Tanzania* Wiley Blackwell: West Sussex.

Murray, A (2013) *Information technology law: The law and the society* Oxford University Press: Oxford.

Mwalimu, C (2009) *The Nigerian legal system* (2007) Peter Lang: Pieterien.

Neethling, J (1976) 'Die Reg op Privaatheid' Unpublished LLD thesis University of South Africa: South Africa.

Neethling, J; Potgieter, JM & Visser, PJ (2005) *Neethling's law of personality* LexisNexis Butterworths: Durban.

Nwamu, GK 'A critical analysis of Freedom of Information Act, 2011' in Azinge, E & Waziri, F (eds) (2012) *Freedom of information law & regulation in Nigeria* Nigerian Institute of Advanced Legal Studies: Lagos.

Odufuwa, F (2012) *What is happening in ICTs in Nigeria: A supply-and demand-side analysis of the ICT sector* researchICTafrica,net available at http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_6_-_Understanding_what_is_happening_in_ICT_in_Nigeria.pdf

Olong, AM (2007) *The Nigerian legal system* Malthouse Press: Ibadan.

Olowu, D (2009) *An integrative rights-based approach to human development in Africa* Pretoria University Law Press: Pretoria.

Park, AEW (1963) *The sources of Nigeria law* Sweet & Maxwell: London.

Pearsall, J(ed) (1999) *The Concise Oxford Dictionary* Oxford University Press: Oxford.

Purtova, N (2012) *Property rights in personal data: A European perspective* Kluwer Law International: The Netherlands.

Rodotà, S 'Data protection as a fundamental right' in Gutwirth, S; Poullet, Y; De Hert, P; De Terwange, C & Nouwt, S (eds)(2009) *Reinventing data protection?* Springer: Heidelberg.

Roos, A 'Data protection' in Van der Merwe, D; Roos, A; Pistorius, T; & Eiselen, S (2008) Information *and communications technology law* LexisNexis: Durban.

Roos, A (2003) 'The law of data (privacy) protection: A comparative and theoretical study' unpublished LLD thesis. University of South Africa: South Africa.

Rouvroy, A & Poullet, Y 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy' Gutwirth, S; Poullet, Y; De Hert, P; De Terwange, C & Nouwt,S (eds)(2009) *Reinventing data protection?* Springer: Heidelberg.

Rowland, D; Kohl, U & Charlesworth, A (2011) *Information technology law* Routledge: New York.

Salami, OO (2015) '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' unpublished LLM thesis, Dalhousie University: Canada.

Scott, MD (2012) *Information technology law* Wolter Kluwer Law & Business: New York.

Shaw, MN (2006) *International law* Cambridge University Press: Cambridge.

Siems, MM (2014) *Comparative law* Cambridge University Press: Cambridge.

Solove, DJ (2004) *The digital person: Technology and privacy in the information age* New York University Press: New York.

Stefanick, L (2011) *Controlling knowledge: Freedom of information and privacy in a networked world* AU Press: Edmonton.

Szekely, I 'The Right to Forgotten: Personal reflections on the fate of personal data in the information society' in Gutwirth, S; Leenes, R; De Hert; P & Poullet, Y (eds) (2012) *European data protection: In good health?* Springer: Heidelberg.

Tobi, N (1996) *Sources of Nigerian l*aw MIJ Professional Publishers: Lagos.

Visser, A & Strachan, D 'South Africa' in Kuschewsky, M (ed) (2012) *Data protection and privacy: Jurisdictional comparisons* Sweet & Maxwell: London.

Wacks, R (1989) *Personal information privacy and the law* Oxford University Press: Oxford.

Wacks, R 'Why there will never be an English common law privacy tort' in Kenyon, AT & Richardson, M (eds) (2006) *New dimensions in privacy law: International and comparative perspectives* Cambridge University Press: Cambridge.

Waziri, F 'Freedom of Information Act 2011: Comparative study with the United State Freedom of Information Act of 1966' Azinge, E & Waziri, F (eds) (2012) *Freedom of information law & regulation in Nigeria* Nigerian Institute of Advanced Legal Studies: Lagos.

Westin, A (1967) *Privacy and freedom* Atheneum: New York.

Westin, A (2015) *Privacy and freedom* IG Publishing: New York.

Wheare, KC (1966) *Modern constitutions* Oxford Paperback University Series: Oxford.

Wilson III, EJ (2006) *The information revolution and developing countries* The MIT Press, Cambridge.

Winn, JK 'Technical standards as data protection regulation' in Gutwirth, S; Poullet, Y; De Hert, P; De Terwange, C & Nouwt, S (eds)(2009) *Reinventing data protection?* Springer: Heidelberg.

Wong, R (2005)'Privacy: Charting its developments and prospects' in Klang, M & Murray, A *Human rights in the digital age* Glasshouse Press: London.

Wong, R (2013) *Data security breaches and privacy in Europe* Springer: Heidelberg.

World Intellectual Property Organisation (WIPO) (2004) *WIPO intellectual property handbook* WIPO publications also available at http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf

Zanfir, G 'Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law' in Gutwirth, S; Leenes, R & De Hert, P (eds) (2014) *Reloading data protection: Multidisciplinary insights and contemporary challenges* Springer: Heidelberg.

Zanfir, G (2013) 'The rights of persons regarding personal data protection' unpublished PhD thesis, University of Craiova, Romania.

Zanfir, G 'Tracing the right to be forgotten in the short history of data Protection law: The "new clothes" of an old right' in Gutwirth, S; Leenes, R & De Hert, P (eds) (2015) *Reforming European data protection law* (2015) Springer: Heidelberg.

Journal articles

Abdulrauf, LA 'Do we need to bother about protecting our personal data? Reflections on neglecting data protection in Nigeria' (2014) 5(2) *Yonsei Law Journal* 67.

Abdulrauf, LA 'Regulating transborder flow of personal information for development in the G77+China' (2015) *Latin American Report* (forthcoming).

Adelola, T; Dawson, R & Batzman, F 'Privacy and data protection in e-commerce in developing nations: Evaluation of different data protection approaches (2015) 6(1&2) *International Journal of Digital Society* 950.

Adesina, AO; Agbele, KK; Februarie, R; Abidoye, AP & Nyongesa, HO 'Ensuring the security and privacy of information in mobile health-care communication systems' (2011) 107 (9/10) *South African Journal of Science* 1.

Akinrinade, B 'Human rights NGOs in Nigeria: Emergence, governmental reaction and the future' (2002) 2 *African Human Rights Law Journal* 110.

Akomolede, TI 'Contemporary legal issues in electronic commerce in Nigeria' (2008) 3 *Potchefstroom Electronic Law Journal* 2/169.

Allan, K & Currie, I 'Enforcing access to information and privacy rights: Evaluating proposals for an Information Protection Regulator for South Africa' (2007) 23 *South African Journal of Human Rights* 563.

Allen, AL 'An ethical duty to protect one's own information privacy?' (2013) 64 *Alabama Law Review* 845.

Araromi, MA 'Regulatory framework of communication sector: A comparative analysis between Nigeria and South Africa' (2015) 23(2) *African Journal of International and Comparative Law* 273.

Austin, LM 'Is consent the foundation of fair information practices? Canada's experience under PIPEDA' (2006) 56 *University of Toronto Law Journal* 181.

Austin, LM 'Privacy and the Question of technology' (2003) 22 *Law & Philosophy* 119.

Austin, LM 'Reviewing PIPEDA: Control, privacy and the limits of fair information practices' (2006) 44 *Canadian Business Law Journal* 21.

Bailey, J 'Systematic government access to private-sector data in Canada' (2012) 2 *International Data Privacy Law* 207.

Banisar, D 'Linking ICTs, the right to privacy, freedom of expression and access to information' (2010) 16 (1) *East African Journal of Peace and Human Rights* 124.

Bennett, CJ 'Adequate data protection by year 2000: The prospects for privacy in Canada' (1997) 11 *International Review of Law and Computers* 79.

Bennett, CJ 'Protecting privacy on the Canadian information highway: Policy developments and regulatory options' (1996) 21 (3-4) *Canadian Journal of Information and Library Science* 1.

Bennett, CJ 'The Privacy Commissioner of Canada: Multiple roles, diverse expectations and structural dilemmas' (2003) 46(2) *Canadian Public Administration* 218.

Bennett, CJ 'The formation of a Canadian privacy policy: The art and craft of lesson-drawing' (1990) 33 *Canadian Public Administration* 551.

Bennett, C & French, M 'The state of privacy in the Canadian State: Fallout from 9/11' (2003) 11(1) *Journal of Contingencies and Crisis Management* 2.

Bennett, CJ; Parsons, CA & Molnar, A 'Real and substantial connections: Enforcing Canadian privacy laws against American social networking companies' (2014) 23(1) *Journal of Library and Information Science* EAP 1.

Bennett, CJ & Raab, CD 'The adequacy of privacy: The European Union Data Protection Directive and the North American response' (1997) 13(3) *The Information Society* 245.

Bergelson, V 'It's personal but is it mine? Towards property rights in personal information' (2003) 37 *UC Davis Law Review* 379.

Bergkamp, L 'The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy' (2002) 18(1) *Computer Law & Security Report* 31.

Bernal, PA 'A right to delete?' (2011) 2 *European Journal of Law and Technology* available at http://ejlt.org/article/view/75/144 (accessed 1 November 2015).

Berzins, C 'Protecting personal information in Canada's private sector: The price of consensus building' (2001-2002) 27 *Queen's Law Journal* 609.

Birnhack, MD 'The EU Data Protection Directive: An engine of a global regime' (2008) 24(6) *Computer Law & Security Report* 508.

Black, RB 'Legislating US data privacy in the context of National Identification Numbers: Models from South Africa and the United Kingdom' (2001) 34 *Cornell International Law Journal* 397.

Blume, P 'The myths pertaining to the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 269.

Blume, P 'Transborder data flow: Is there a solution in sight' (2000) 8(1) *International Data Privacy Law* 65.

Burchell, J 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13(1) *Electronic Journal of Comparative Law* 1.

Bygrave, LA 'Determining applicable law pursuant to European data protection legislation' (2000) 16 *Computer Law & Security Report* 252.

Bygrave, LA 'Data protection pursuant to the right to Privacy' (1998) 6(3) *International Journal of Law and Information Technology* 247.

Bygrave, LA 'The place of privacy in data protection law' (2001) 24 *UNSW Law Journal* 277.

Bygrave, LA 'Privacy and data protection in an international perspective' (2010) *Stockholm Institute for Scandinavian Law* 164.

Calaguas, MJ 'South African Parliament enacts comprehensive data protection law: An overview of the Protection of Personal Information Bill' (2013) 3 *Africa Law Today* 1.

Caruana, MM & Cannataci, JA 'European Union privacy and data protection principles: Compatibility with culture and legal frameworks in Islamic states' (2007) 16(2) *Information & Communications Technology Law* 99.

Cate, FH & Litan, R 'Constitutional issues in information privacy' (2002) 9(1) *Michigan Telecommunications and Technology Law Review* 35.

Cerda Silva, AJ 'Internet freedom is not enough: Towards an internet based on human rights' (2013) 18 *SUR International Journal of Human Rights* 17.

Christiansen, E 'Transformative constitutionalism in South Africa: Creative uses of Constitutional Court authority to advance substantive justice' (2010) 13 *The Journal of Gender, Race & Justice* 575.

Clarke, R 'Privacy impact assessment: Its origins and development' (2009) 25(2) *Computer Law & Security Review* 123.

Cockfield, AJ 'The state of privacy laws and privacy encroaching technologies after September 11: A two-year report card on the Canadian government' (2003-2004) 1 *University of Ottawa Law and Technology Journal* 325.

Cronje, FS 'A synopsis of proposed data protection legislation in SA' (2009) 4(4) *Journal of Digital Forensics, Security and Law* 43.

Currie, I 'Scrutiny: South Africa's Promotion of Access to Information Act' (2003) 9(1) *European Public Law* 59.

Dada, JA 'Human rights under the Nigerian Constitution: Issues and problems' (2012) 2(12) *International Journal of Humanities and Social Science* 33.

De Hert, P & Papakonstantinou, V 'The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28(2) *Computer Law & Security Review* 130.

De Hert, P & Papakonstantinou, V 'Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency?' (2013) 9(2) *I/S: A Journal of Law and Policy for the Information Society* 271.

Dove, ES; Black, L, Avard, D & Knoppers, BM 'Charting the privacy landscape in Canadian paediatric biobanks' (2013) 20 *Health Law Journal* 1.

Du Plessis, LM 'The evolution of constitutionalism and the emergence of a constitutional jurisprudence in South Africa: An evaluation of the South African Constitutional Court's approach to constitutional interpretation' (1999) 62 *Saskatchewan Law Review* 299.

Eskridge, WN & Frickey, PP 'Quasi-constitutional law: Clear statement rules as constitutional lawmaking' (1992) 45 *Vanderbilt Law Review* 593.

Fishleigh, J 'Is someone watching you? Data privacy and protection: Current issues' (2015) 15(1) *Legal Information Management* 61.

Flaherty, DH 'On the utility of constitutional rights to privacy and data protection' (1990-1991) 41 *Case Western Reserve Journal of International Law* 831.

Fialová, E 'Data portability and informational self-determination' (2014) 8(1) *Masaryk University Journal of Law and Technology* 45.

Fombad, CM 'African Bills of Rights in a comparative perspective' (2011) 17(1) *Fundamina* 33.

Fromholz, JM 'The European Union Data Privacy Directive' (2000) 15 *Berkeley Technology Law Journal* 461.

Froomkin, AM 'The death of privacy?' (2000) 52 *Stanford Law Review* 1461.

Fuster, GG & Geller, R 'The fundamental right of data protection in the European Union: In search of an uncharted right' (2012) 26(1) *International Review of Law, Computers & Technology* 73.

Fuster, GG & Gutwirth, S 'Opening up personal data protection: a conceptual controversy' (2013) 29(5) *Computer Law & Security Review* 531.

Garrie, DB & Wong, R 'Demystifying clickstream data: A European and US perspective' (2006) *Emory International Law Review* 563.

Geist, M & Homsi, M 'Outsourcing our privacy?: Privacy and security in a borderless commercial world (2005) 54 *University of New Brunswick Law Journal* 272.

Gillis, P 'The Privacy Act: A legislative history and overview' (1987) 119 *Canadian Human Rights Yearbook* 119.

Gomes dé Andrade, NN 'Oblivion: The right to be different from oneself' (2012)13 *Revista de Internet, Derecho y Politica* 122.

Greenleaf, G '76 Global data privacy laws' (September 2011) 112 *Privacy Law and Business Special Report* 11.

Greenleaf, G 'Asia-Pacific data privacy: 2011, year of revolution?'(2011) *Kyung Hee Law Journal.*

Greenleaf, G 'Independence of data privacy authorities (Part I): International standards' (2012) 28 *Computer & Security Review* 3.

Greenleaf, G 'Independence of data privacy authorities: International standards and Asia-Pacific experience' (2012) 28 (1&2) *Computer & Security Review.*

Greenleaf, G "'Modernising' Data Protection Convention 108: A safe basis for a global privacy treaty?" (2013) 29(4) *Computer Law & Security Review* 430.

Greenleaf, G 'Morocco and Uruguay start Convention 108's journey to global privacy Treaty' (2013) 122 *Privacy Laws & Business International Report* 20.

Greenleaf, G 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2014) 23(1) *Journal of Law, Information & Science* 8.

Greenleaf, G 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108' (2012) 2(2) *International Data Privacy Law* 68.

Greenleaf, G & Georges, M 'The African Union's Data Privacy Convention: A major step toward global consistency' (2014) 131 *Privacy Laws & Business International Report* 18.

Guzman, AT & Meyer, TL 'International soft-law' (2010) 2(1) *Journal of Legal Analysis* 171.

Hamann, B & Papadopoulos, S 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) 47(1) *De Jure* 42.

Haque, AZ & Le, MH 'Privacy year in review: Canada's Personal Information and Protection and Electronic Documents Act and Japan's Personal Information Act' (2004-2005) 1 *I/S: A Journal of Law and Policy for the information Society* 477.

Hildebrandt, M & Tielemans, L 'Data protection by design and technology neutral law' (2013) 29(5) *Computer Law and Security Review* 509.

Hirsch, DD 'The law and policy of online privacy: Regulation, self-regulation or co-regulation?' (2011) 34 *Seattle University Law Review* 439.

Hon, WK; Millard, C & Walden, I "The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing" (2011) 1(4) *International Data Privacy Law* 211.

Hornung, G 'Regulating privacy enhancing technologies: Seizing the opportunity of the future European data protection framework' (2013) 26(1-2) *The European Journal of Social Science Research* 181.

Hornung, G & Schnabel, C 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25(1) *Computer Law & Security Review* 84.

Jaeger, PT; Bertot, JC & McClure, CR 'The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act' (2003) 20(3) *Government Information Quarterly* 295.

Jemilohun, BO 'An appraisal of the institutional framework for data protection in the UK, USA, Canada and Nigeria' (2015) 1(1) *Journal of Asian and African Social Science and Humanities* 8.

Jemilohun, BO 'Legislating for data protection in Nigeria: Lessons from UK, Canada and India' (2010) 1 *Akungba Law Journal* 116.

Jemilohun, BO & Akomolede, TI 'Legislating for cyberspace: Challenges for the Nigeria legislature' (2015) 38 *Journal of Law, Policy and Globalization* 129.

Jemilohun, BO & Akomolede, TI 'Regulations or legislations for data protection in Nigeria? A call for a clear legislative framework' (2015) 3(4) *Global Journal of Politics and Law Research* 1.

John, U 'Privacy: A forgotten right in Tanzania' (2012) *Tanzania Lawyer* 72.

Kashan, S 'The USA Patriot Act: Impacts on freedom and civil liberties' (2009) 7 *ESSAI* 86.

Kettemann, MC 'The UN Human Rights Council Resolution on Human Rights on the Internet: Boost or Bust for Online Human Rights Protection?' (2012) 1 *Human Security Perspectives* 145.

Killander, M 'How international human rights law influences domestic law in Africa' (2013) 17 *Law, Democracy & Development* 378.

Kim, W 'Cloud computing: Today and tomorrow' (2009) 8(1) *Journal of Object Technology* 65.

Kokott, J & Sobotta, C 'The distinction between privacy and data privacy in the jurisprudence of the CJEU and EctHR' (2013) 3(4) *International Data Privacy Law* 222.

Koops, B 'The trouble with European data protection law' (2014) 4(4) *International Data Privacy Law* 250.

Kuner, C 'An international legal framework for data protection: Issues and prospects' (2009) 25(4) *Computer Law & Security Review* 307.

Kuner, C 'The European Union and the search for an international data protection framework' (2014) 2(1) *Groningen Journal of International Law* 55.

Kong, L 'Data protection and transborder data flow in the European global context' (2010) 21(2) *The European Journal of International Law* 441.

Kotschy, W 'The proposal for a new General Data Protection Regulation – problems solved?'(2014) 4(4) *International Data Privacy Law* 274.

Kusamotu, A 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by Article 25 of European Union Directive 95/46' (2007) 16(2) *Information & Communications Technology Law* 149.

Levin, A & Nicholson, MJ 'Privacy law in the United States, the EU and Canada: The Allure of the middle ground' (2005) 2 *University of Ottawa Law & Technology Journal* 357.

Lindsay, D 'An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law' (2005) 29 *Melbourne University Law Review* 131.

Lockwood, BB; Finn, J & Jubinsky, G'Working paper for the committee of experts on limitation provisions' (1985) 7(1) *Human Rights Quarterly* 35.

Lynskey, O 'Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78(5) *The Modern Law Review* 522.

Lynskey, O 'Deconstructing data protection: The 'added value' of a right to data protection in the EU legal order' (2014) 63(3) *International and Comparative Law Quarterly* 569.

Makulilo, AB "Data protection regimes in Africa: too far from the European 'adequacy' standard?" (2013) 3(1) *International Data Privacy Law* 42.

Makulilo, AB 'Myth and reality of harmonization of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 78.

Makulilo, AB 'Nigeria's Data Protection Bill: Too many surprises' (2012) 120 *Privacy Law and Business International Report* 25.

Makulilo, AB '"One size fits all": Does Europe impose its data protection regime on Africa?' (2013) 7 *Datenschutz und Datensicherheit* 447.

Makulilo, AB "'Peel off the mask': Enforcement of Data Protection Act in Mauritius' (2014) 12 *Datenschutz und Datensicherheit* 845.

Makulilo, AB 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) *International Data Privacy Law* 163.

Makulilo, AB 'Privacy in mobile money: Central banks in Africa and their regulatory limits' (2015) 0 *International Journal of Law and Technology*.

Masete, NT 'The challenges in safeguarding financial privacy in South Africa' (2012)7(3) *Journal of International Commercial Law and Technology* 248.

Mayer-Schönberger, V 'Demystifying Lessig' (2008) *Wisconsin Law Review* 713.

McClennan, J & Schick, V '"O, privacy" Canada's importance in the development of the international data privacy regime' (2007) 38 *Georgetown Journal of International Law* 669.

McQuoid-Mason, DJ 'Invasion of privacy: Common law v constitutional delict—does it make a difference?' (2000) 227 *Acta Juridica* 227.

McQuoid-Mason, DJ 'Consumer protection and the right to privacy' (1982) 15(2) *The Comparative and International Law Journal of Southern Africa* 135.

Mhlaba, SL 'The efficacy of international regulation of transborder data flows: The case for clipper chip' (1995) 12 *Government Information Quarterly* 353.

Millard, D 'Hello, POPI? On cold calling, financial intermediaries and advisors and the Protection of Personal Information Bill' (2013) 76(4) *Tydskrif vir hedendaagse Romeins-Hollandse Reg (THRHR)* 604.

Moshell, R '…and then there was one: The outlook for a self-regulatory United states amidst a global trend toward comprehensive data protection' (2004-2005) 37 *Texas Tech Law Review* 357.

Ncube, C 'A comparative analysis of Zimbabwean and South African data protection systems' (2004) 2 *The Journal of Information, Law and Technology* available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_2/ncube/

Ncube, CB 'Watching the watcher: Recent developments in privacy regulation and cyber-surveillance in South Africa' (2006) 3(4) *SCRIPT-ed* 344.

Neethling, J 'Data protection and juristic persons' (2008) 71 *Tydskrif vir hedendaagse Romeins-Hollandse Reg* (*THRHR)* 71.

Neethling, J 'Features of the Protection of Personal Information Bill 2009, and the law of delict' (2012) 75 *Tydskrif vir hedendaagse Romeins-Hollandse Reg*. (*THRHR)* 241.

Neethling, J 'Personality rights: A comparative overview' (2005) 38(2) *Comparative and International Law Journal of Southern Africa* 210.

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

Newman, DE 'European Union and United States personal information privacy and human rights philosophy- is there a match?' (2008) 22 *Temple International and Comparative Law Journal* 307.

Nisker, J 'PIPEDA: A constitutional analysis' (2006) 85 *The Canadian Bar Review* 317.

Nova, TD 'The future face of the worldwide data privacy push as a factor affecting Wisconsin business dealing with consumer data' (2004) 22(3) *Wisconsin International Law Journal* 769.

Nwauche, ES 'The right to privacy in Nigeria' (2007) 1(1) *Review of Nigerian Law and Practice* 64.

Oba, AA "'Neither fish nor fowl': Area courts in the Ilorin emirate in Northern Nigeria" (2008) 58 *Journal of Legal Pluralism* 69.

Oba, AA 'The African Charter on Human and Peoples' Rights and ouster clauses under the military regimes in Nigeria: Before and after September 11' (2004) 4(2) *African Human Rights Law Journal* 275.

Obute, PC 'ICT laws in Nigeria: Planning and regulating a societal journey into the future' (2014) 17(1) *Potchefstroom Electronic Law Journal* 420.

Okogbule, NS 'Access to justice and human rights protection in Nigeria' (2005) 3(2) *SUR-International Journal of Human Rights* 94.

Olayemi, OJ 'Combating the menace of cybercrime' (2014) 3(6) *International Journal of Computer Science and Mobile Computing* 980.

Olayemi, OJ 'A socio-technological analysis of cybercrime and cyber security in Nigeria'6 (3) *International Journal of Sociology and Anthropology* (2014) 116.

Olinger, HN; Britz, JJ & Olivier, MS 'Western privacy and/or *Ubuntu?* Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa' (2007) 39(1) *International Information & Library Review* 31.

Oraegbunam, IKE 'Crime and punishment in igbo customary law: The challenge of Nigerian criminal jurisprudence' (2010) 6 (1) *New Journal of African Studies* 53.

Owasanoye, B & Akanle, A 'ICTs, freedom of information and privacy rights in Nigeria: A legal analysis' (2010) 16(1) *East African Journal of Peace & Human Rights* 99.

Oyetayo, Y 'Principles based regulations: A model for legal reform in the Nigerian insurance industry' (2015) 59(1) *Journal of African Law* 64.

Oyewunmi, AO 'The ICT revolution and commercial sectors in Nigeria: Impacts and legal interventions' (2012) 5 *British Journal of Arts and Social Sciences* 234.

Pantuvo, JS, Naguib, R & Wickramasinghe, N 'Towards implementing a nationwide electronic health record system in Nigeria' (2011) 3 *International Journal of Healthcare Delivery Reform Initiatives* 39.

Phillipson, G 'Transforming breach of confidence? Towards a common law right of privacy under the Human Rights Act' (2003) 66 *Modern Law Review* 726.

Picker, RC 'Competition and privacy in Web 2.0 and the cloud' (2008) 103 *North-western University Law Review Colloquy* 1.

Piper, T 'The Personal Information Protection and Electronic Documents Act: A lost opportunity to democratize Canada's "technological society"' (2000) 23 *Dalhousie Law Journal* 256.

Poullet, Y 'The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206.

Purtova, N 'Property rights in personal data: Learning from the American discourse' (2009) 25 *Computer Law & Security Review* 507.

Roos, A 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* 400.

Roos, A 'Personal data protection in New Zealand: Lessons for South Africa (2008) 4 *Potchefstroom Electronic Law Journal* 62.

Roos, A 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *The South African Law Journal* 375.

Rosen, J 'The right to be forgotten' (2012) 64 *Stanford Law Review Online* 88.

Rotondo, E 'The legal effect of EU Regulations' (2013) 29 (4) *Computer & Security Report* 437.

Schartum, DW 'Designing and formulating data protection laws' (2008)18 *International Journal of Law and Information Technology* 1.

Schwartz, B 'Canada's new privacy law: Strategies for compliance' (2002) 2 *Asper Review of International Business and Trade Law.* 125.

Schwartz, PM & Solove, DJ 'Reconciling personal information in the United States and European Union' (2014) 102 *California Law Review* 877.

Schwartz, PM & Solove, DJ 'The PII problem: Privacy and a new concept of personally identifiable information' (2011) 86 *New York University Law Review* 1814.

Shaffer, GC & Pollack, MA 'Hard vs. soft law: Alternatives, compliments, and antagonists in international governance' (2010) 94 *Minnesota Law Review* 706.

Shimanek, AE 'Do you want milk with those cookies?: Complying with the Safe Harbor privacy principles' (2001) 26 *The Journal of Corporation Law* 455.

Siegel, A; Denny, W; Poff, KW; Larose, C; Hale, R & Hintze, M 'Survey of privacy law developments in 2009: United States, Canada, and the European Union (2009) 65(1) *The Business Lawyer* 285.

Sluijs, JP; Larouche; P & Sauter, W 'Cloud computing in the EU policy sphere interoperability, Vertical integration and the internal market' (2012) 3 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 12.

Smith, A 'Privacy and the sale of customer lists in South African insolvency law. Some issues reconnoitred' (2004) 16 *South African Mercantile Law Journal* 598.

Solove, DJ 'Conceptualizing privacy' (2002) 90 *California Law Review* 1092.

Solove, DJ 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745.

Solove, DJ 'Privacy and power: Computer databases and metaphors for information privacy' (2001) 53 *Stanford Law Review* 1393.

Spaeth, JM; Plotkin, MJ & Sheets, CS 'Privacy, Eh! The impact of Canada's Personal Information Protection and Electronic Documents Act on transnational business' (2002) 4 *Vanderbilt Journal of Entertainment Law and Practice* 28.

Stefanick, L 'Outsourcing and transborder data flows: The challenge of protecting personal information under the shadow of the USA Patriot Act' (2007) 73 *International Review of Administrative Sciences* 531.

Stein, P '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).

Strauss, J & Rogerson, KS 'Policies for online privacy in the United States and the European Union' 19 *Telematics and Informatics* (2002)173.

Swire, P & Lagos, Y 'Why the right to data portability likely reduces consumer welfare: Antitrust and privacy critiques' (2013) 72 *Maryland Law Review* 335.

Tamò, A & George, D 'Oblivion, erasure and forgetting in the digital age' (2014) 2 *Journal of Intellectual Property, Information Technology & E-commerce* 71.

'Trend report: Information technology in Nigeria' (2012) *African Journal of Economics* available at http://africanjoe.com/?p=1 (accessed 1 November 2015).

Tzanou, M 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right' (2013) 3(2) *International Data Privacy Law* 88.

Uvin, P "From the right to development to the rights-based approach: How 'human rights' entered development" (2007) 17(4-5) *Development in Practice* 597-606.

Van der Bank, CM 'The right to privacy - South African and comparative perspectives' (2012) 1(6) *European Journal of Business and Social Sciences* 77.

Van der Merve, D 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17(1) *Potchefstroom Electronic Law Journal* 296.

Van der Sloot, B 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 307.

Victor, JM 'The EU General Data Protection Regulation: Toward a property regime for protecting data Privacy' (2013) 123(2) *The Yale Law Journal* 513.

Visser, C 'The protection of personal information in broadcasting: The effect of the Protection of Personal Information Bill on freedom of expression' (2011) 27 *South African Journal of Human Rights* 331.

Walby, K "'Little England? The rise of open-street closed-circuit television surveillance in Canada" (2006) 4 *Surveillance & Society* 29.

Weber, RH 'The digital future -A challenge for privacy?' (2015) 31(2) *Computer Law & Security Review* 238.

Wong, R 'Data protection online: Alternative approaches to sensitive data? (2007) 2(1) *Journal of International Commercial Law and Technology* 9.

Wong, R 'The Data Protection Directive 95/46/ EC: Idealisms and realisms' (2012) 26 *International Review of Law, Computers & Technology* 229-254.

Wright, D 'The state of the art in privacy impact assessment' (2012) 28 *Computer Law & Security Review* 54.

Xanthoulis, N 'The right to oblivion in the information age: A human rights-based approach' (2013) 10 *US China Law Review* 84.

Yusuff, AOA 'Legal issues and challenges in the use of security (CCTV) cameras in public places: Lessons from Canada' (2011) 23 *Sri Lanka Journal of International Law* 33.

Zalnieriute, M 'An international constitutional moment for data privacy in the times of mass surveillance' (2015) 23(2) *International Journal of Law and Information Technology* 99.

Zalnieriute, M 'Book review: Paul Bernal, Internet privacy rights: Rights to protect autonomy' (2015) 31 *Computer Law and Security Review* 312.

Zanfir, G 'The right to data portability in the context of the EU data protection reform' (2012) 3 (2) *International Data Privacy Law* 149.

Zarsky, TZ 'Desperately seeking solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society' (2004) 56(1) *Maine Law Review* 13.

Zimmerman, RK 'The way the "cookies" crumble: Internet privacy and data protection in the twenty-first century' (2002) 4 *Legislation and Public Policy* 439.

Reports, documents and (working) papers

'A Report of the online debate on Africa Union Convention on Cyber security (AUCC)' submitted to the African Union Commission (AUC) http://www.iitpsa.org.za/wp-content/uploads/2014/02/REPORT-ON-OF-THE-ONLINE-DEBATE-ON-AFRICA-UNION-CONVENTION-ON-CYBERSECURITY.pdf (accessed 1 November 2015).

APEC Cross-border Privacy Enforcement Arrangement (CPEA). http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx (accessed 1 November 2015).

Arowosaiye, YI 'The new phenomenon of phishing, credit card fraud, identity theft, internet piracy and Nigeria criminal law' paper presented at the 3rd Conference on

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

Article 29 Data Protection Working Party 'Opinion 4/2007 on the concept of personal data' http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (accessed 1 November 2015).

Article 29 Data Protection Working Party 'Discussion document: First orientations on transfers of personal data to third countries: Possible ways forward in assessing adequacy' XV D/5020/97-EN final WP4 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf (accessed 1 November 2015).

Article 29 Data Protection Working Party 'Working document on protection issues related to intellectual property' January 18, 2005 available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp104_en.pdf (accessed 24 January 2016).

Article 29 Data Protection Working Party 'Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive' DG XV D/5025/98 WP 12 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf (accessed 31 November 2015).

Article 29 Data Protection Working Party 'Opinion 15/2011 on the definition of consent' available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (accessed 1 November 2015).

Bennett, C 'Regulating privacy in Canada: An analysis of oversight and enforcement in the private sector' (1996).

Bennett, CJ 'The Office of the Privacy Commissioner of Canada: Regulator, educator, consultant and judge'. Paper presented at conference on "Two sides of the coin: Relations between parliamentary agencies and the public service." Canadian centre for management development, March 2002.

Council of Europe 'Final document on the modernisation of Convention 108' available at https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04_rev2_En.pdf (accessed 1 November 2015).

Council of Europe Convention explanatory report http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm (accessed 1 November 2015).

Council of the European Union 'The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act' 22 November 2006 http://ec.europa.eu/justice/policies/privacy/docs/adequacy/canada_st15644_06_en.pdf (accessed 1 November 2015).

De Hert, P & Schreuders, E 'The Relevance of Convention 108', 33, 42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19-20 November 2001.

Department of Communication and Department of Justice 'Privacy and computers' a report of a Task Force established jointly by the Department of Communications/ Department of Justice (1972).

Department of International Law, Permanent Council of the Organization of American States 'Comparative study: Data protection in the Americas' OEA/Ser.G CP/CAJP-3063/12, 3 April 2012. Available online at http://scm.oas.org/doc_public/ENGLISH/HIST_12/CP28327E04.doc (accessed 1 November 2015).

Department of Justice 'The offices of the information and privacy commissioners: The merger and related issues' http://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/ip/p2.html#ftn5 (accessed 1 November 2015).

Dutta, S; Dutton, W & Law, G 'The new internet world, a global perspective on freedom of expression, privacy, trust and security online' the global information technology report 2010-2011 9 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1916005 (accessed 1 November 2015).

EPIC 'Privacy and human rights report 2006 of the Federal Republic of Nigeria' available at http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Federal-3.html#Heading9594 (accessed 1 November 2015).

European Commission 'A comprehensive approach on personal data protection in the European Union' Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM (2010) 609 final 2 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (accessed 1 November 2015).

European Commission 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments' JLS/2008/C4/011 – 30-CE-0219363/00-28 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1636706 (accessed 1 November 2015).

European Commission (EC) 'Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act' http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0002&from=EN (accessed 1 Noember 2015).

European Commission 'Privacy enhancing technologies (PETs): The existing legal framework' available at http://europa.eu/rapid/press-release_MEMO-07-159_en.htm (accessed 1 November 2015).

European Commission Directorate-General Justice, Freedom and Security 'Comparative study on different approaches to new privacy challenges, in particular I the light of technological development' Final report available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf (accessed 1 November 2015).

European Union 'Study on the legal analysis of a single market for information society: New rules for a new age?'

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=833 (accessed on 1 November 2015).

Explanatory Memorandum of the proposed General Data Protection Regulation, context of the Proposal, COM (2012) 11 final, 2. Also available online http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011 (accessed 1 November 2015).

EPIC & Privacy International 'privacy and human rights report' (2006) 10 edition http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Contents.html (accessed 1 November 2015).

Explanatory memorandum to the Guidelines http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation (accessed 1 November 2015).

Explanatory report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1980) available at http://conventions.coe.int/Treaty/en/Reports/Html/108.htm (accessed on 1 November 2015).

Ferraud-Ciandet, N 'Privacy and data protection in eHealth: A comparative approach between South African and French legal systems' (2010) IST-Africa 2010 conference proceeding P Cunningham & M Cunningham (eds) *International Information Management Corporation* 2010. Also available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=5753017 (accessed 1 November 2015).

Freedom House 'Nigeria' 2013 https://freedomhouse.org/report/freedom-net/2013/nigeria (accessed 1 November 2015).

Gauthronet, S & Drouard, E 'Unsolicited commercial communications and data protection' (January 2001) available at http://ec.europa.eu/justice/data-protection/document/studies/files/20010202_spamstudy_en.pdf (accessed 1 November 2015).

'Government accountability for personal information: Reforming the Privacy Act' June 2006 https://www.priv.gc.ca/information/pub/pa_reform_060605_e.asp (accessed 1 November 2015).

House of Commons Standing Committee on Human rights and the Status of Persons with disabilities 'Privacy rights and new technologies: Consultation package' in *Privacy: Where Do We Draw the Line?* Appendix i, 1 available at https://www.priv.gc.ca/information/02_06_03d_e.pdf (accessed 1 November 2015).

Industry Canada & Justice Canada 'Protection of personal information: Building Canada's information economy and society' Discussion paper 24 January 1998.

Iglezakis, I 'The right to be forgotten in the Google Spain Case (case C-131/12): A clear victory for data protection or an obstacle for the internet?' paper presented at the 4th International conference on information law (2014).

Lawson, I 'Privacy and the information highway, regulatory options for Canada' (1996).

Mendel, T; Puddephatti, A; Wenger, B; Hawtin, D & Torres, N 'Global survey on internet privacy and freedom of expression' (2012) available at

http://unesdoc.unesco.org/images/0021/002182/218273e.pdf (accessed 1 November 2015).

'Nigeria's National Broadband Plan 2013-2018' a submission by the presidential committee on broadband available at http://www.researchictafrica.net/countries/nigeria/Nigeria_National_Broadband_Plan_2013-2018.pdf (accessed 1 November 2015).

NIMC 'Proposed privacy policy' https://www.nimc.gov.ng/sites/default/files/pia_policy.pdf (accessed on 1 November 2015).

Nigerian National Policy for Information Technology available at http://www.researchictafrica.net/countries/nigeria/Nigerian_National_Policy_for_Information_Technology_2000.pdf (accessed 1 November 2015).

Nigerian National Policy for Information Technology (IT) 'Use IT' available at http://www.functionx.com/nitpa/nigeria/ITPOLICY.PDF (accessed 1 November 2015).

OECD Ministerial Declaration on the protection of privacy on global networks privacy international 'A Borderless World: Realising the Potential of Global Electronic Commerce' 7-9 October 1998. http://www.oecd.org/internet/ieconomy/1840065.pdf (accessed 1 November 2015).

OECD Ministerial Meeting on the Future of the Internet Economy. http://www.oecd.org/document/8/0,3343,en_2649_34487_40863240_1_1_1_1,00.html (accessed 1 November 2015).

OECD 'The OECD Privacy Framework' (2013) available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed 1 November 2015).

OECD 'Thirty years after the OECD Privacy Guidelines' (2011) http://www.oecd.org/sti/ieconomy/49710223.pdf (accessed 1 November 2015).

OECD 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy' available at http://www.oecd.org/internet/ieconomy/38770483.pdf (accessed 1 November 2015).

Office of the Privacy Commissioner of Canada 'Privacy Legislation in Canada' Fact sheets https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp (assessed 1 November 2015).

Office of the Privacy Commissioner of Canada 'The case for reforming the Personal Information Protection and Electronic Documents Act' https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp (accessed 1 November 2015).

Office of the Privacy Commissioner of Canada, 'Guidelines for Processing Personal Data Across Borders' (2009), http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf (accessed 1 November 2015).

Office of the Privacy Commissioner of Canada 'Presentation to E-Commerce and Privacy implementing the new law in the public and private sectors' February 21, 2000

https://www.priv.gc.ca/media/sp-d/02_05_a_000221_2_e.asp (accessed 1 November 2015).

Office of the Privacy Commissioner of Canada 'Submission to the Standing Committee on Public Safety and National Security of the House of Commons' March 5, 2015. https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp (accessed 1 November 2015).

Office of the Privacy Commissioner of Canada 'Privacy Act reforms' https://www.priv.gc.ca/parl/2008/parl_080429_02_e.asp (accessed 1 November 2015).

PIPEDA Report of Findings #2014-009 https://www.priv.gc.ca/cfdc/2014/2014_009_0210_e.asp (accessed 1 November 2015).

Privacy Commissioner of Canada, Annual Report to Parliament, 2004-2005, http://www.privcom.gc.ca/information/ar/200405/200405_pa_e.asp (accessed 1 November 2015).

Privacy International 'Privacy and human rights: An international survey of privacy laws and practice' http://gilc.org/privacy/survey/intro.html (accessed 1 November 2015).

'Reports by UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' 28 December 2009 A/HRC/13/37. Available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf (accessed 1 November 2015)

Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/08-10-17_Strasbourg_international_standards_EN.pdf (accessed 1 November 2015).

Robinson, N; Graux, H; Botterman, M & Valer, L 'Review of the European Data Protection Directive' (Technical report), RAND Corporation (May 2009) available at http://www.rand.org/pubs/technical_reports/TR710.html (accessed 1 November 2015).

South African Law Reforms Commission 'Privacy and data protection report' (2009) http://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf (accessed 1 November 2015).

South African Law Reform Commission 'Privacy and data protection project' 124 Issue Paper October 2005 available at http://www.justice.gov.za/salrc/dpapers/dp109.pdf (accessed 1 November 2015).

Stoddart, J 'Government accountability for personal information: Reforming the Privacy Act' available at https://www.priv.gc.ca/information/pub/pa_reform_060605_e.asp (accessed 1 November 2015).

Task Force on Privacy and Computers 'Privacy and Computers' a report of a Task Force established jointly by Department of Communications/Department of Justice (Ottawa: Information Canada, 1972).

Therrien, D 'Senate standing committee on National Security and Defence (SECD) on Bill C-44, An Act to amend the Canadian Security Intelligence Service Act and other Acts' https://www.priv.gc.ca/parl/2015/parl_20150309_e.asp (accessed 1 November 2015).

Treasury Board of Canada Secretariat 'Policy on privacy protection' http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=HTML (accessed 1 November 2015).

UN Human Rights Council's Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet 2012.

United Nations General Assembly 'Reports by UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', 28 December 2009 A/HRC/13/37 http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf (accessed 3 September 2015).

US Department of Health Education and Welfare (DHEW) 'Record computers and the rights of citizens' Report of the Secretary's Advisory Committee on Automated Personal Data Systems http://www.justice.gov/opcl/docs/rec-com-rights.pdf (accessed 1 November 2015).

Newspapers

Aginam, E 'At last, Senate passes Cyber Crime Bill into law' *Vanguard newspaper* 5 November 2014.

Amaefule, E 'Nigeria recorded 52 % internet growth in 2014 – Minister' *Punch* 18 May 2015.

'Buhari orders INEC, FRSC, NPC to harmonise biometric data' *Vanguard* 11 August 2015.

Chiejina, A 'Jonathan finally signs National Health Bill into law' *Business day* (accessed 1 November 2015).

Emmanuel, O 'EXCLUSIVE: Jonathan awards $40 Million contract to Israeli company to monitor computer, internet communication by Nigerians' *Premium Times* 25 April 2013.

Ezigbo, O 'Nigeria: Bill to safeguard personal information underway' *Thisday Newspaper* 24 February 2013.

'Internet usage on Nigeria's telecoms networks hits 93 million –NCC' *Leadership* 12 September 2015.

Idoko, C 'Identity theft: FG proposes law on personal information, data protection' *Nigerian Tribune Newspaper* 22 February 2013.

'NCC fines four GSM operators N1bn' *The Punch newspaper* 13 May 2012.

'Nobody can hack into INEC database - Jega' *Punch Newspaper* January 21 2015.

Nurudeen, NA 'Nigeria: "Data Breaches cost increased to U.S. $3.8 Million in one year' *Daily trust* 3 June 2015.

Online resources

'7 foundational principles' http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/ (accessed 1 November 2015).

'About APEC' http://www.apec.org/About-Us/About-APEC.aspx (accessed 1 November 2015).

'About the OECD' http://www.oecd.org/about/ (accessed 1 November 2015).

'About INEC' http://www.inecnigeria.org/?page_id=14 (accessed 1 November 2015).

Abuja: Where are the CCTV cameras?' http://www.thisdaylive.com/articles/abuja-where-are-the-cctv-cameras-/141195/ (accessed 1 November 2015).

Adeniyi, As 'The need for data protection law in Nigeria' https://adeadeniyi.wordpress.com/2012/07/18/the-need-for-data-protection-law-in-nigeria-2/ (accessed 1 November 2015).

African Declaration 'About the initiative' http://africaninternetrights.org/about/ (accessed 1 November 2015).

Akinsuyi, FF 'Data protection and privacy laws in Nigeria: A trillion dollar opportunity!!' http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2598603 (accessed 3 September 2015).

Akinsuyi, FF 'Data protection legislation for Nigeria: The time is now!' http://www.datalaws.com/pdf/article02.pdf (accessed 3 September 2015).

Akunyili, D 'ICT and e-government in Nigeria: Opportunities and challenges' address by the Hon. Minister of Information and Communications, Prof Dora Akunyili, at the world congress on information technology, Amsterdam, the Netherlands, 25th-27th may 2010. Available at https://goafrit.wordpress.com/2010/06/12/ict-and-e-government-in-nigeria-prof-akunyili/ (accessed 3 September 2015).

APEC 'Member economies' http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (accessed 1 November 2015).

'Asia-Pacific: Canada's joining of APEC CBPRs will 'strengthen the system'http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3615 (accessed 1 November 2015).

Article 19 'Nigeria Personal Information and Data Protection Bill' (2013) available online in http://www.article19.org/resources.php/resource/3683/en/nigeria:-personal-information-and-data-protection-bill (accessed 1 November 2015).

'Backup and restore' http://windows.microsoft.com/en-ZA/windows7/products/features/backup-and-restore (1 November 2015).

Balboni, P; Mccorry, K & Snead, WD 'Cloud computing. Benefits, risks and recommendations for information security' (2009) European Networks and Information Security Agency (ENISA) https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cloud%20Computing%20Security%20Risk%20Assessment%20%282%29.pdf (accessed 1 November 2015).

Bakibinga, EM 'Managing electronic privacy in the telecommunication sub-sector: The Ugandan perspective' (2004)

http://www.thepublicvoice.org/events/capetown04/bakibinga.doc (accessed 1 November 2015).

Banks, T '2013 OECD Privacy Guidelines- will Canada respond?' http://www.lexology.com/library/detail.aspx?g=c6df76c5-e982-4761-ba38-5cb49a08167e (accessed 1 November 2015).

Barroso, IMC & Goulven, K 'A rights-based revolution' http://www.undatarevolution.org/2014/10/14/rights-based-revolution/ (accessed 1 November 2015).

Bennett, C 'The role of a Privacy Commissioner and the qualifications of Daniel Therrien: What parliament should be asking' June 2014 available at http://www.colinbennett.ca/2014/06/the-role-of-a-privacy-commissioner-and-the-qualifications-of-daniel-therrien-what-parliament-should-be-asking/ (accessed 1 November 2015).

'C-51 Anti-terrorism Bill "excessive" Privacy Commissioner says' http://www.cbc.ca/news/politics/c-51-anti-terrorism-bill-excessive-privacy-commissioner-says-1.2984376 (accessed 1 November 2015).

Cavoukian, A 'Privacy by design' https://www.ipc.on.ca/images/resources/privacybydesign.pdf (accessed 1 November 2015).

Cavoukian, A 'Privacy by design in law, policy and practice: A white paper for regulators, decision makers and policy makers' available at https://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf (accessed 1 November 2015).

'Central Bank of Nigeria introduces Bank Verification Number (BVN)' http://nairabrains.com/2014/10/central-bank-of-nigeria-introduces-bank-verification-number-bvn/ (accessed 1 November 2015).

Chart of signatures and ratifications of Treaty 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures (accessed 1 November 2015).

Chinn, MD & Fairlie, RW 'ICT use in the developing world: An analysis of differences in computer and internet penetration' Working paper, National Bureau of Economic Research (July 2006) available at http://www.nber.org/papers/w12382.pdf (accessed 1 November 2015).

'Circular on the acceleration of bank verification number (BVN) project' available at http://www.cenbank.org/Out/2014/BPSD/CIRCULAR%20ON%20ACCELERATION%20ON%20BVN2.pdf (accessed 1 November 2015).

Clarke, R 'Introduction to dataveillance and information privacy, definitions of terms' http://www.rogerclarke.com/DV/Intro.html (accessed 1 November 2015).

'Comparing the co-regulatory model, comprehensive laws and the sectoral approach' available at https://www.cippguide.org/2010/06/01/comparing-the-co-regulatory-model-comprehensive-laws-and-the-sectoral-approach/ (accessed 1 November 2015).

Council of Europe http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp(accessed 1 November 2015).

Council of Europe 'The Council in brief' http://www.coe.int/en/web/about-us/who-we-are (accessed 1 November 2015).

'Credit Bureau Association of Nigeria' http://www.mfw4a.org/news/news-details/article/2869/credit-bureau-association-of-nigeria.html (accessed 1 November 2015).

Currie, I 'The Protection of Personal Information Act and its impact on freedom of information', (2010) http://www.opendemocracy.org.za/wp-content/uploads/2010/10/The-Protection-of-Personal-Information-Act-and-its-Impact-on-Freedom-of-Information-by-Iain-Currie.pdf (accessed 1 November 2014).

'Data protection laws of the world: South Africa' available at http://dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=ZA (accessed 1 November 2015).

Data Security Council of India 'Strengthening data protection through co-regulation' available at http://cis-india.org/internet-governance/blog/strengthening-privacy-protection.pdf (accessed 1 November 2015).

European Commission 'Frequently asked questions on the Commission's adequacy finding on the Canadian Personal Information Protection and Electronic Documents Act' http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq_en.htm (accessed 1 November 2015).

'Facebook South Africa user numbers' http://businesstech.co.za/news/internet/72266/facebook-south-africa-user-numbers/ (accessed 1 November 2015).

Flaherty, DH 'Reflections on reforms of Federal Privacy Act' (2008) https://www.priv.gc.ca/information/pub/pa_ref_df_e.pdf (accessed 1 November 2015).

Fuster, GG & Gutwirth, S 'Ethics, law and privacy: Disentangling law from ethics in privacy discourse' proceedings of the 2014 IEEE International Symposium on ethics in science, technology and engineering, 23-24 May 2014, Chicago. Available at http://works.bepress.com/cgi/viewcontent.cgi?article=1161&context=serge_gutwirth (accessed 1 November 2015).

Frontline Protection of Human rights defenders 'Nigeria: Defending human rights: Not everywhere not every right international fact finding mission' April 2010. Available at http://www.omct.org/files/2010/05/20688/nigeria_mission_report.pdf (accessed 1 November 2015).

'Framework for global electronic commerce' http://www.w3.org/TR/NOTE-framework-970706 (accessed 1 November 2015).

Geist, M 'Why the Digital Privacy Act undermines our privacy: Bill s-4 risks widespread warrantless disclosure' April 10 2014 http://www.michaelgeist.ca/2014/04/s-4-post/ (accessed 1 November 2015).

Greenleaf, G 'Global tables of data privacy laws and bills' (3rd Ed, June 2013). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875 (accessed 1 November 2015).

Gwagwa, A & Wilton, A '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 1 November 2015).

Holmes, N 'Canada's federal privacy laws' (2008) http://www.parl.gc.ca/Content/LOP/researchpublications/prb0744-e.htm (accessed 1 November 2015).

Hornung, G Abstract of the presentation for the Interparliamentary Committee Meeting titled 'The reform of the EU Data Protection framework – Building trust in a digital and global world'. Session II – Harmonised and strengthened data protection rights and principles for an interconnected world, 9/10 October 2012, Brussels available http://www.europarl.europa.eu/document/activities/cont/201210/20121008ATT53088/20121008ATT53088EN.pdf (accessed 1 November 2015).

'How the EU works' http://europa.eu/about-eu/ (accessed on 1 November 2015).

Human Rights Watch (HRW) 'The role of the Independent National Electoral Commission (INEC)' http://www.hrw.org/legacy/backgrounder/africa/nigeria0407/5.htm (accessed 1 November 2015).

Heyder, M 'The APEC Cross-Border Privacy Rules – Now that we've built it, will they come? *Privacy Perspectives* September 4, 2014 https://privacyassociation.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come/ (accessed 1 November 2015).

'iCloud: iCloud storage and backup overview' http://support.apple.com/kb/ph12519(accessed 1 November 2015).

'ICT (Information and communication technology – technologies)' http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies (accessed 1 November 2015).

Industry Canada 'About us' http://www.ic.gc.ca/eic/site/icgc.nsf/eng/h_00007.html (accessed 1 November 2015).

'INEC's database is fortified and cannot be hacked – Jega' http://whatsupnaija.info/inecs-database-is-fortified-and-cannot-be-hacked-jega/ (accessed 1 November 2015).

InfoWorld.com 'The notorious nine: Cloud computing top threats in 2013' https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf (accessed 1 November 2015).

Internet Live Stat 'Africa' http://www.internetworldstats.com/africa.htm (accessed 1 November 2015).

Internet Live Stat 'Internet Usage Statistics for Africa' http://www.internetworldstats.com/stats1.htm#africa (accessed 1 December 2015). (accessed 1 December 2015).

Internet World Stats 'Usage and population statistics' http://www.internetworldstats.com/stats1.htm (accessed 1 November 2015).

ITU 'Measuring the information society report' (2014) available at https://www.itu.int/en/ITU-

D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf (1 November 2015).

Izuogu, CE 'Data protection and other implications of the ongoing SIM card registration process' http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665 (accessed 1 November 2015).

'Judicial activism law & legal definition' http://definitions.uslegal.com/j/judicial-activism/ (accessed 1 November 2015).

'Junk mail' http://www.businessdictionary.com/definition/junk-mail.html#ixzz3QhTdUAmC (accessed 1 November 2015).

Kazeem, A 'Legal aspects of e-payment in government' http://www.nigerianlawguru.com/articles/general/LEGAL%20ASPECTS%20OF%20E-PAYMENT%20IN%20GOVERNMENT.pdf (accessed 1 November 2015).

Keith, BC 'Privacy north of the border: 10 things you should know about Canadian personal information laws' (2004) 14 *American Business Association Business Law Section* available at http://apps.americanbar.org/buslaw/blt/2004-11-12/keith.shtml (accessed 1 November 2015).

Kelley, K 'This powerful spy software is being abused by governments around the world' http://www.businessinsider.com/countries-with-finfisher-spying-software-2013-5#ixzz31vYCYV4X (accessed 1 November 2015).

Mantelero, A 'U.S. concern about the European right to be forgotten and free speech: Much ado about nothing?'(2012) *Contratto E Impresa / Europa* 727 available at http://rememberingandforgetting.wikispaces.com/file/view/US+Concern+about+the+European+Right+to+Be+Forgotten+and+Free+Speech.pdf (accessed 1 November 2015).

Meglena Kuvena speech delivered at Roundtable on Online Data Collection, Targeting and Profiling Brussels, 31 March 2009. Available at http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (accessed 1 November 2015).

Milo, D & Palmer, G 'South Africa- New comprehensive data privacy law passed' *Linklaters* 31 January 2014 available at http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-News-31-January-2014/Pages/SouthAfrica-New-comprehensive-data-privacy-law-passed.aspx (accessed 1 November 2015).

Nyamu-Musembi, C & Cornwall, A 'What is the "rights-based approach" all about? Perspectives from international development agencies' working paper series, 234 Brighton: IDS available at http://opendocs.ids.ac.uk/opendocs/handle/123456789/4073#.Vc2TC7Vu6Wg (accessed 1 November 2015).

Lithwick, D 'Bill S-4: An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act (2014) 1 http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/2/s4-e.pdf (accessed 1 November 2015).

Luck, R 'POPI- Is South Africa keeping up with international trends' (May 2014) 541 *De Rebus* 45 also available at http://reference.sabinet.co.za/webx/access/electronic_journals/derebus/derebus_n541_a26.pdf (accessed 1 November 2015).

Momentum Health 'International student application form' http://www.ingwehealth.co.za/Files/(20141110113238%20AM)%20STUDENTHEALTH005_0115E_International_Student_Application_form_fillable.pdf (accessed 1 November 2015).

Nahra, KJ 'A new HIPAA era emerges, privacy in focus' (2009) 3-4, available at http://www.escaladeit.com/sites/default/files/A_New_HIPAA_Era_Emerges.pdf (accessed 1 November 2015).

Nigeria Communications Commission http://www.ncc.gov.ng/ (accessed 1 November 2015).

'Nigeria: Adoke lauds NIMC Proposed Draft Bill on Information, Data Protection' http://allafrica.com/stories/201302220301.html (accessed 1 November 2015).

'Nigeria becomes Africa's biggest economy' BBC News Business, 6 April 2014, available at http://www.bbc.com/news/business-26913497 (accessed 1 November 2015).

NIMC 'About us' https://www.nimc.gov.ng/?q=about-us (accessed 1 November 2015)

NITDA 'About us' http://www.nitda.gov.ng/about.html (accessed 1 November 2015).

'OAU/AU Treaties, Conventions, Protocols & Charters' http://www.au.int/en/treaties (accessed 1 November 2015).

Office of the Privacy Commissioner www.priv.gc.ca.

Office of the Privacy Commissioner of Canada 'About the Office of the Privacy Commissioner' https://www.priv.gc.ca/au-ans/index_e.asp (accessed 1 November 2015).

Office of the Privacy Commissioner of Canada 'The necessary rebirth of the Privacy Act' 29 November 2013 https://www.priv.gc.ca/media/sp-d/2013/sp-d_20131129_02_e.asp (accessed 1 November 2015).

'OECD work on privacy' http://www.oecd.org/sti/ieconomy/privacy.htm (accessed 1 November 2015).

Oguntimehin, J 'Implications of Nigeria's National ID card' http://www.iafrikan.com/2014/09/30/nigeria-national-id-card/#sthash.aDBRkrnA.dpuf (accessed 1 November 2015).

Olagunju, T 'Mr President and the National Assembly: Data protection for Nigerians first' http://saharareporters.com/2014/09/02/mr-president-and-national-assembly-data-protection-nigerians-first (accessed 1 November 2015).

Olaleye, B 'Is Data Protection Act inconsequential?' http://www.gbooza.com/group/nigeriapolitics/forum/topics/is-data-protection-act#ixzz3ITCPwCy3 (accessed 1 November 2015).

'Platform for Privacy Preferences (P3P) Project' http://www.w3.org/P3P/ (accessed 1 November 2015).

Press Release Speech Viviane Reding 'Justice for Growth makes headway at today's Justice Council' SPEECH/13/29, 18.01.2013 available at http://europa.eu/rapid/press-release_SPEECH-13-29_en.htm (accessed 1 November 2015).

'Privacy by design' http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design (accessed 1 November 2015).

'Privacy is dead – Get over it- Steve Rambam' https://www.youtube.com/playlist?list=PL8C71542205AA51E5(accessed 1 November 2015).

Radwanski, G letter to the Hon. David Collenette, Minister of Transport https://www.priv.gc.ca/media/nr-c/02_05_b_011130_e.asp (accessed 1 November 2015).

Remling, A 'iCloud nude leaks: 26 celebrities affected in the nude photo scandal' http://www.ibtimes.com/icloud-nude-leaks-26-celebrities-affected-nude-photo-scandal-1692540 (accessed 1 November 2015).

'Rights abuses complicate US support for Nigeria' http://www.dw.de/rights-abuses-complicate-us-support-for-nigeria/a-17648303 (accessed 1 November 2015).

SALRC 'About' http://www.justice.gov.za/salrc/about.html (accessed 1 November 2015).

Sebatindira, S 'A glimpse into the emergent e-commerce in Nigeria' http://www.consultancyafrica.com/index.php?option=com_content&view=article&id=1754:a-glimpse-into-the-emergent-e-commerce-in-nigeria&catid=82:african-industry-a-business&Itemid=266 (accessed 3 September 2015).

Solove, DJ "Why Privacy Matters Even if You Have 'Nothing to Hide'" http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/ (Accessed 1 November 2015).

Shorter, A 'Concepts of social justice in traditional Africa' http://www.afrikaworld.net/afrel/atr-socjustice.htm (accessed 1 November 2015).

Stoddart, J 'Data protection and security: A transnational discussion' an address on May 5, 2006 available at https://www.priv.gc.ca/media/sp-d/2006/sp-d_060505_e.asp (accessed 1 November 2015).

'Subscriber Statistics: Monthly Subscriber Data' Nigerian Communications Commission http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&Itemid=73 (accessed 1 November 2015).

'The 2007 international privacy ranking: State of privacy map' http://www.democraticunderground.com/discuss/duboard.php?az=view_all&address=132x3911587 (accessed 1 November 2015).

'The case for reforming the Personal Information Protection and Electronic Documents Act' May 2013 https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp (accessed 1 November 2015).

'The information technology landscape in Canada' http://www1.american.edu/carmel/sa0565a/leg_env.htm (accessed 1 November 2015).

Treasury Board of Canada Secretariat 'About the Treasury Board' http://www.tbs-sct.gc.ca/tbs-sct/abu-ans/tb-ct/abu-ans-eng.asp (accessed 1 November 2015).

Udo, B 'CBN sets new deadline for bank customer's verification' *Premium Times* http://www.premiumtimesng.com/business/169879-cbn-sets-new-deadline-for-bank-customers-verification.html (accessed 1 November 2015).

University of South Africa (UNISA) 'Compliance with the Protection of Personal Information (POPI) Act' http://www.unisa.ac.za/news/index.php/2015/03/compliance-with-the-protection-of-personal-information-popi-act/ (accessed 1 November 2015).

'What is observer status?' http://www.coe.int/en/web/portal/what-is-observer-status (accessed 1 November 2015).

'What's my user agent' http://whatsmyuseragent.com/WhatsAUserAgent (accessed 1 November 2015).

World Economic Forum (WEF) *Personal data: The emergence of a new asset class* (2011) available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed 1 November 2015).

XDS Credit Bureau. http://www.xdscreditbureau.com/ (accessed 1 November 2015).

XDS Credit Bureau 'Our products and services' http://www.xdscreditbureau.com/product&services.php (accessed 1 November 2015).

'Yes, Celebs had their iCloud accounts hacked. No, you shouldn't shut yours off' http://www.forbes.com/sites/markrogowsky/2014/09/03/the-celeb-hack-has-people-telling-you-to-turn-off-cloud-backup-ignore-them/ (accessed 1 November 2015).