Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime

Andrew Ubaka Iwobi[*]

Abstract: *Nigeria's progress towards becoming a full-fledged member of the global information society has been impeded by its inability to devise a credible data protection regime. This Article focuses on Nigeria's recent attempts to regulate the processing of personal information within its jurisdiction. This inquiry is pursued through the analytical prism of legal transplantation. The Article exposes serious failings within the Nigerian legislative process and casts a critical eye on the injudicious and indiscriminate borrowing of foreign laws undertaken by Nigeria's regulatory authorities in their quest to join the ever-growing ranks of the nations with their own data protection laws. This Article also provides a veritable lesson in the potential dangers of legal transplantation.*

---

[*] LL.B (Jos), Ph.D (Birmingham), Senior Lecturer and Course Director for the LL.M E-Commerce module, College of Law, Swansea University. The author is grateful to participants in the Swansea University Institute of Shipping and Trade Law (IISTL) Research Seminar December 2, 2015 for their invaluable comments on an earlier draft of this Article.

I. INTRODUCTION

The preamble to the EU General Data Protection Regulation states that:

> Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.[1]

The rapid technological advances and globalizing tendencies that have swept through the European Union have also become increasingly evident in various parts of Africa in the past decade.[2] Like the Member States of the European Union, African countries like Nigeria are currently grappling with the complex and manifold challenges to individual privacy, which have come to the fore in the modern information age.[3] Nigeria has recently embarked on the task of regulating the processing of personal information within its technological borders.[4] As part of this process, the Nigerian legal system has gone down the well-trodden path of legal transplantation in an effort to devise a sound legislative regime for the protection of such information.[5]

---

[1] Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), COM (2012) 11 final 5419/1/16 (Apr. 8, 2016), pmbl. 6, http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf.

[2] *See Technology Will Drive Growth in Africa Over the Next Five Years*, IT TECH NEWS AFRICA (Jan. 22, 2015), http://www.itnewsafrica.com/2015/01/technology-will-drive-growth-in-africa-over-the-next-five-years/ ("Africa is booming and a lot of this economic growth stems from investment in technology . . . . Nairobi [Kenya] and Lagos [Nigeria] . . . are already well on the way to becoming global tech hotspots."); *see also Technology in Africa the Pioneering Continent*, THE ECONOMIST (Apr. 25, 2015), http://www.economist.com/news/middle-east-and-africa/21649516-innovation-increasingly-local-pioneering-continent ("A continent that has long accepted technological hand-me-downs from the West is increasingly innovating for itself . . . . Technology is opening up African markets that have long been closed or did not previously exist . . . . Africa's innovation revolution is still in its infancy. But it is likely to gain pace.").

[3] LEE A. BYGRAVE, DATA PRIVACY LAWS: AN INTERNATIONAL PERSPECTIVE 80 (2014) ("Africa is now home to some of the most prescriptively ambitious data privacy initiatives"); Alex Boniface Makulilo, *Data Protection Regimes in Africa: Too Far From the European 'Adequacy' Standard?,* 3 INT. DATA PRIVACY L. 42, 42 (2013) ("[After] four decades of the development of data protection laws, the world has witnessed data protection regimes finally arriving in Africa.").

[4] *See* Alex B. Makulilo, *Nigeria's Data Protection Bill: Too Many Surprises,* 120 PRIVACY L. & BUS: DATA PROTECTION & PRIVACY INFO. WORLDWIDE 25 (2012); *see also* Bernard Oluwafemi Jemilohun & Timothy Ifedayo Akomolede, *Regulations or Legislation for Data Protection in Nigeria? A Call for a Clear Legislative Framework,* 3 GLOBAL J. OF POL. & L. RES. 1 (2015), http://www.eajournals.org/wp-content/uploads/Regulations-or-Legislation-for-Data-Protection-in-Nigeria1.pdf.

[5] *See* discussion *infra* Parts IV.C–IV.E.

The basic premise of this Article is that Nigeria's regulatory authorities have utilized the mechanism of legal transplantation in the fledgling field of data protection in a manner that has been detrimental to the nation's quest for an appropriate statutory framework. Their approach has been desultory and ill-conceived, and their various pieces of draft legislation reveal an alarming lack of in-depth knowledge of the transplanted laws and an absence of the sophisticated mindset needed to render those laws amenable to the Nigerian context. This is unfortunate because it exposes serious failings within the Nigerian legislative process, which will inevitably hinder the nation's progress towards the legal modernization that is vital to compete with other nations in the highly complex and rapidly evolving technological sphere.

This Article will explore legal transplantation in three main parts. The first part sets the scene by briefly explaining the phenomenon of legal transplantation, with particular emphasis on its importance as a mechanism for legislative reform, its utility within the sphere of data protection, and its historical and contemporary relevance within the Nigerian legal system. The second part examines the vital role of modern digital technologies, such as the internet, in the transmission of vast quantities of electronic data across the globe. Part two highlights Nigeria's growing receptivity towards these new technologies. Nigeria is not alone in this regard. The severe threat to individual privacy arising from the unfettered transmission of such data has not only placed the protection of personal data firmly on the legislative agenda in a large number of countries, but has also provided the impetus for a host of international initiatives designed to harmonize the data protection regimes of these countries.[6] The third section of this Article consists of a critical review of several pieces of draft legislation on data protection currently circulating in Nigeria. This review reveals their drafters have unabashedly plagiarized the U.K. Data Protection Act 1998[7] (U.K. DPA 1998) and, in one instance, the Canadian Personal Information Protection and Electronic Documents Act 2000.[8] In the process, the Nigerian legislature has been oblivious to the difficulties inherent in the operation of these statutes in their original settings, failed to take account of significant changes that have either been made to these statutes or are imminent in their home jurisdictions and given very little thought to the suitability of these statutes within the Nigerian context.

---

[6] *See infra* Part III.B.

[7] Data Protection Act, 1998, c 29 (Eng.) [hereinafter DPA 1998].

[8] Personal Information Protection and Electronic Documents Act, 2000 S.C, c 5 (Can.) [hereinafter PIPEDA].

II. LEGAL TRANSPLANTATION AND ITS MANIFESTATION WITHIN THE NIGERIAN LEGAL SYSTEM

A. Legal Transplantation as a Legislative Tool

Legal transplantation entails "the transfer of laws and institutional structures across geopolitical or cultural borders."[9] It has been pointed out that legal transplants are "commonly observed around the world . . . [and] can range from the wholesale adoption of entire systems of law to the copying of a single rule."[10] Alan Watson, who has justifiably been described as "the guru of legal transplants,"[11] argues with characteristic boldness that one of the most startling and obvious characteristics of legal rules is "the apparent ease with which they can be transplanted from one system to another"[12] and asserts that "massive successful borrowing is commonplace in law."[13]

This theme has also been taken up by Kahn-Freund, who points out that legal developments overseas have become increasingly relevant to law making and law reform, and that lawmakers routinely look abroad for new ideas and techniques.[14] Kahn-Freund's reference to the propensity of lawmakers to look abroad for inspiration reflects the fact that legislation has become the principal means by which laws are transplanted. It has accordingly been acknowledged that even though various institutions within a legal system may be involved in the transplantation of laws, such transplantation is "far more often a result of decisions by national legislators."[15]

Legal transplantation within the legislative arena has been portrayed in a positive light by various commentators who have drawn particular attention to the procedural efficiency that can be achieved through legislative borrowing. Watson has remarked in this connection, "borrowing rules and structures from elsewhere . . . can be the cheapest and most efficient way of changing the

---

[9] JOHN GILLESPIE, TRANSPLANTING COMMERCIAL LAW REFORM: DEVELOPING A 'RULE OF LAW' IN VIETNAM 3 (2006).

[10] Hideki Kanda & Curtis J. Milhaupt, *Re-Examining Legal Transplants: The Director's Fiduciary Duty in Japanese Corporate Law*, 51 AM. J. COMP. L. 887, 887 (2003); *see also* GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES 12 (2014).

[11] Helen Xanthaki, *Legal Transplants in Legislation: Defusing the Trap,* 57 INT'L & COMP. L.Q. 659, 660 (2008).

[12] Alan Watson, *Comparative Law and Legal Change,* 37 CAMBRIDGE L.J. 313, 313 (1978).

[13] Alan Watson, *Legal Transplants and European Private Law*, 4 ELECTRONIC J. COMP. L. (2004).

[14] Otto Kahn-Freund, *On Uses and Misuses of Comparative La*w, 37 MOD. L. REV. 1, 2 (1974) (Kahn-Freund has been eulogized as one of the greatest jurists of the 20th century); *see Otto Kahn-Freund*, 42 MOD. L. REV. 609 (1979) (his views on legal transplantation have therefore been accorded considerable weight in the scholarly literature on the topic).

[15] Jorg Fedtke, *Legal Transplants*, *in* ELGAR ENCYCLOPEDIA OF COMPARATIVE LAW 550, 550 (Jan M. Smits ed., 2d ed. 2012).

law."[16] Similarly, another scholar asserted, "[i]t is . . . easier and simply cheaper to copy an existing rule than to reinvent the wheel. In addition to saving part of the time and cost of drafting legislation, practical experience with a foreign model will often be available at no extra expense."[17] This dimension of legislative borrowing is also emphasized by Xanthaki, who has written extensively on issues pertaining to the quality of legislation and the transferability of legislative solutions from one legal system to another. Xanthaki opines that borrowing from foreign jurisdictions is a means of developing legislation quickly and effectively and insists that "[i]n an era of tight parliamentary schedule[s] where drafters are asked to produce bills at unprecedented speed, drafting teams must be afforded the luxury of seeking ready solutions with proven results elsewhere, in similar and different legal systems".[18]

However, Xanthanki has argued that effectiveness (rather than efficiency) is the principal virtue pursued by legislative drafters all over the world. Xanthanki asserts that "effectiveness is the platform of transferability of laws, institutions and legislative solutions."[19] Effectiveness in this particular context refers to the extent to which the observable attitudes and behaviors of the target population correspond to, and are the consequence of, the norms prescribed by the legislator.[20] It is incumbent on legislators who set out to borrow from other legal systems to scrutinize the substantive rules and principles of the legislation they are seeking to transplant and the policies that underpin this legislation in a rigorous and painstaking manner, before it is formally enacted. In the absence of such scrutiny, it is highly unlikely that the transplanted legislation will operate effectively in its new setting. As shown below, the Nigerian government does not appear to have appreciated the importance of such scrutiny in its recent efforts to establish a legislative framework for the regulation of personal data.

---

[16] Watson, *supra* note 12, at 326.

[17] Fedtke, *supra* note 15, at 550; *see also* Loukas A. Mistelis, *Regulatory Aspects, Globalization, Harmonization, Legal Transplants, and Law Reform - Some Fundamental Observations*, 34 INT'L LAWYER 1055, 1067 (2000) ("[t]he argument is strong that there is no need for legislators to struggle to reinvent the wheel when others have dealt with the same issues."); Kanda & Milhaupt, *supra* note 10, at 889 ("legal transplants . . . are a cheap, quick and potentially fruitful source of new law.").

[18] Xanthanki, *supra* note 11, at 661–62.

[19] Helen Xanthaki, *On Transferability of Legislative Solutions: The Functionality Test*, *in* DRAFTING LEGISLATION: A MODERN APPROACH 1, 16 (Constantin Stefanou & Helen Xanthaki eds., 2008); *see also* Luzius Mader, *Evaluating the Effects: A Contribution to the Quality of Legislation*, 22 STAT. L. REV. 119, 125–27 (2001).

[20] Xanthaki, *supra* note 19; Mader, *supra* note 19. Factors that determine the effectiveness of legislation include the nature of the substantive rules and principles embodied in the legislation, the type of language in which these rules are formulated, the manner and extent to which they have been communicated to the target population, and the mechanisms and procedures through which they are enforced.

B. Colonization and Harmonization as Instruments of Legal Transplantation

Watson characterizes the process of "borrowing from another system [as] the most common form of legal change."[21] In bygone days, such legal change was often brought about through the process of conquest and colonization. This mode of transplantation is exemplified by the wholesale transplantation of English law into Nigeria by the British colonial authorities from the mid-nineteenth century onwards.[22]

Nevertheless, it is also the case that large-scale legal transfers are equally possible without colonization.[23] A great deal of legal transplantation occurs voluntarily, in situations where a society's laws have become outmoded, ossified, arbitrary, or abusive. Transplants may also be needed when the society encounters some new problem or subject matter that its existing laws do not address properly, thereby prompting its lawmakers to look elsewhere for legal edification.[24] It has also been pointed out that "[o]ther . . . reasons for using legal transplants include the harmonization of law within the framework of international agreements."[25] This particular mode of legal transplantation is exemplified by the extensive program of legal harmonization that has taken place across much of present-day Europe, under the aegis of what is now the European Union (hereinafter the EU).[26]

In fact, since the 1980s, various harmonization projects have been actively pursued in the field of data protection by different sub-global, regional and sub-regional organizations.[27] Commenting on this trend, Greenleaf, who is a leading authority on global data privacy, explains that the concept of data protection or data privacy "is now relatively well defined 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."[28] He also emphasizes that such international agreements "have contributed a great deal to

---

[21] Alan Watson, *Legal Change, Sources of Law and Legal Culture*, 131 U. PA. L. REV. 1121, 1125 (1983).

[22] *See infra* Part II.D.

[23] GILLESPIE, *supra* note 9, at 4.

[24] John Witte Jr., *Canon Law in Lutheran Germany: A Surprising Case of Legal Transplantation in* LEX ET ROMANITAS: ESSAYS FOR ALAN WATSON 181 (Michael Hoeflich ed., 2000).

[25] Fedtke, *supra* note 15, at 550.

[26] *See* Witte, *supra* note 24, at 182; *see also* Hakeem Rizk, Comment, *Fundamental Right or Liberty? Online Privacy's Theory for Co-Existence with Social Media*, 56 HOW. L.J. 951, 963 (2013) ("The European Union is guided by a political and economic mission to standardize the laws of all member countries in an effort to function as one unified market . . . .").

[27] For example, the Organization for Economic Cooperation and Development [hereinafter OECD]; the Council of Europe [hereinafter CoE], the Asia-Pacific Economic Cooperation forum, the EU, the African Union, and the Economic Community of West African States [hereinafter ECOWAS].

[28] GREENLEAF, *supra* note 10, at 5.

development of consistency of national data privacy laws."[29] The consistency alluded to by Greenleaf is indicative of the considerable amount of transplantation through the process of legal harmonization that has taken place throughout the world in the sphere of data protection in recent decades. It is for that reason, as he suggests, that data protection provides "an interesting case study" of the phenomenon of legal transplantation.[30]

C. The Feasibility of Legal Transplants

Xanthaki is critical of legislative drafters who borrow legal solutions and legislative texts from foreign jurisdictions and generally pay little heed to established theories and controversies concerning the legitimacy and feasibility of legal transplants. She points out that

> [t]his creates problems of inapplicability of the transplanted law within the receiving national legal context. In turn, inapplicability leads to failure of the purpose of the transplanted law. Failure of purpose signifies not only collapse of the intended regulation but also wastage of resources in legislating and enforcing an inevitably failing legislation and, perhaps more importantly, the negligent creation of the false or fraudulent impression that the problem is adequately addressed.[31]

Many other scholars also vigorously dispute Watson's core message that "the transplanting of legal rules is socially easy."[32] Watson considers transplantation to be socially easy because he firmly believes that "legal rules may be very successfully borrowed [even] where the relevant social, economic, geographical and political circumstances of the recipient are very different from those of the donor system," and that "the recipient system does not require any real knowledge of the social, economic, geographical and political context of the origin and growth of the original rule."[33] Cairns, who has recently undertaken a wide-ranging and highly illuminating review of the burgeoning literature on legal transplants, observes that there have been persistent and regular criticisms of Watson's work in this field and is especially struck by the fact that "the idea of 'legal transplants' or 'transplantation of

---

[29] *Id.* at 6; *see also* Alex B. Makulilo, *Myth and Reality of Harmonisation of Data Privacy Policies in Africa,* 31 COMPUT. L. & SEC. REV. 78, 78 (2015) ("Modern technologies have made it possible for more personal information to cross national borders than ever before . . . . Concomitantly in [the] 1970s and 1980s harmonisation of data privacy policies became a policy agenda.").

[30] GREENLEAF, *supra* note 10, at 12.

[31] Xanthaki, *supra* note 11, at 659.

[32] ALAN WATSON, LEGAL TRANSPLANTS 95 (2d ed. 1993).

[33] Alan Watson, *Legal Transplants and Law Reform*, 92 L.Q. REV. 79, 80–81 (1976).

laws' seems so obvious to some scholars, while others remain skeptical."[34] Cabrelli and Siems also highlight the antipathy towards Watson.[35] They point out that culturalists, like Legrand[36] have unequivocally rejected the Watsonian standpoint, while contextualists like Kahn-Freund have also called it into question.[37] The disagreement between Watson and Legrand has been particularly pronounced. Their divergent positions are encapsulated by the "split between those [like Watson] who proclaim the feasibility of transplantation as a device of legal change, and those [like Legrand] who claim that they are impossible."[38]

Smits opines that Legrand's claim that legal transplantation is impossible is "too radical," and "has not been recognized as insightful"[39]; while Nelken characterizes it as "unhelpful."[40] Nelken concedes that "if by 'legal transplants' we mean the attempts to use laws and legal institutions to reproduce identical meanings and effects in different cultures, then this is indeed impossible."[41] He however points out that Watson has never sought to argue otherwise, thus implying Legrand's criticism of Watson was not particularly well directed. Nelken maintains that "[i]t can hardly be gainsaid that legal transfers are possible, are taking place, have taken place and will take place."[42] Similarly, Harding asserts that "it seems as if Watson's theory of legal transplantation . . . is made out to a remarkable extent"[43] and "the evidence of successful legal transplants of almost every conceivable kind is powerful."[44]

---

[34] John W. Cairns, *Watson, Walton, and the History of Legal Transplants*, 41 GA. J. INT'L & COMP. L. 637, 639 (2013).

[35] David Cabrelli & Mathias Siems, *Convergence, Legal Origins, and Transplants in Comparative Corporate Law: A Case-based and Qualitative Analysis*, 63 AM. J. COMP. L. 109, 124–25 (2015).

[36] *See generally* Pierre Legrand, *The Impossibility of 'Legal Transplants'*, 4 MAASTRICHT J. EUR. & COMP. L. 109–24 (1997); Pierre Legrand, *What "Legal Transplants"?, in* ADAPTING LEGAL CULTURES 55–70 (David Nelken & Johannes Feest eds., 2001).

[37] Kahn-Freund, *supra* note 14, at 13–27 (using a range of examples drawn from such disparate fields as family law, legal institutions, and procedures and the law of labor relations, Kahn-Freund seeks to illustrate the risk of rejection inherent in any attempt to transplant a pattern of law outside the environment of its origin).

[38] Kanda & Milhaupt, *supra* note 10, at 889.

[39] Jan Smits, *On Successful Legal Transplants in a Future Ius Commune Europaeum, in* COMPARATIVE LAW IN THE 21ST CENTURY 141 (Andrew Harding & Esin Örücü eds., 2002).

[40] David Nelken, *Comparatists and Transferability, in* COMPARATIVE LEGAL STUDIES: TRADITIONS AND TRANSITIONS 437, 442 (Pierre Legrand & Roderick Munday eds., 2003).

[41] *Id.* at 442.

[42] *Id.* at 443.

[43] Andrew Harding, *Comparative Law and Legal Transplantation in South East Asia: Making Sense of the "Nomic Din", in* ADAPTING LEGAL CULTURES 199, 213 (David Nelken & Johannes Feest eds., 2001).

[44] *Id.* at 218–19.

Contextualists like Kahn-Freund have adopted a more nuanced approach. While not wholly averse to the notion that laws may be transplanted between legal systems, he does not share Watson's conviction that such transplantation is easy to accomplish. Kahn-Freund asserts in this connection that there are varying "degrees of transferability"[45] and that "we cannot take for granted that rules or institutions are transplantable."[46] Therefore, it is incumbent on legislators contemplating the use of foreign legal models "[to] ask what chances there are that the new law will be adjusted to the [host] environment and what are the risks that it will be rejected."[47] He opines that this "requires a knowledge not only of the foreign law, but also of its social, and above all its entire political, context"[48] and insists that "[t]he use of comparative law for practical purposes becomes an abuse . . . if it . . . ignores this context of the law."[49] What Kahn-Freund means is that comparative law can serve as a tool for law reform since those who prepare new legislation often avail themselves of legal rules and institutions developed in foreign countries, but that if it is simply taken for granted that such foreign rules and institutions are inherently transplantable and due cognizance is not taken of the possibility that they may be rejected, this constitutes an abuse or misuse of the discipline of comparative law. This line of reasoning has more recently been reiterated by Niglia who asserts that "[a]ccording to [the] line of scholarship initiated by Otto Kahn-Freund, a 'misuse' of the comparative law method takes place whenever the actors involved in the legislative process transplant foreign rules in their own legal system with little regard for the rules' context."[50] Such misuse has occurred in the Nigerian legal system where the regulatory elite have uncritically adopted foreign legislation such as the Data Protection Act ("DPA") 1998[51] and the Personal Information Protection and Electronic Documents Act ("PIPEDA") 2000,[52] without giving serious thought to the fact that social, economic, and political conditions in Nigeria differ substantially from those in England and Canada, from where these two pieces of legislation emanated.[53]

---

[45] Kahn-Freund, *supra* note 14, at 6.

[46] *Id.* at 27.

[47] *Id.* at 6.

[48] *Id.* at 27.

[49] *Id.*

[50] Leone Niglia, *Of Harmonization and Fragmentation: The Problem of Legal Transplantation in the Europeanization of Private Law,* 17 MAASTRICHT J. EUR. & COMP. L. 116, 117 (2010).

[51] Data Protection Act, 1998, c 29 (Eng.).

[52] Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5 (Can.).

[53] *See infra* at Parts IV.C–IV.E.

D. Legal Transplantation Within the Nigerian Legal System

The dispersal of English law to the distant corners of the British Empire, including the territory that eventually became the Colony and Protectorate of Nigeria, reflects the magnitude of transplantation.[54] English law was introduced into the territory by Ordinance No.3 of 1863, two years after Nigeria's former capital, Lagos, was formally annexed.[55] Lagos served as a staging point for the colonization of other parts of Nigeria in the decades that followed. As part of this process, the 1863 Ordinance was eventually superseded by the Supreme Court Ordinance of 1914, which extended the operation of English law to the rest of Nigeria.[56] This latter Ordinance provided that "[s]ubject to the terms of this or any other Ordinance, the common law, the doctrines of equity and the statutes of general application which were in force in England on the first of January 1900, shall be in force within the jurisdiction of the court."[57]

The template for the reception of English law laid down in these early Ordinances has remained in effect in post-independent Nigeria (albeit with certain textual variations between the versions in force in the thirty-six states of the Federation). This resonates with Watson's view that a notable characteristic of legal rules, when transplanted from one system or society to another, is the longevity that they usually exhibit within their new environment.[58] This view is clearly borne out by the fact that even though a century and a half has elapsed since English law gained its first foothold in Nigeria, its importance has scarcely diminished in the intervening years. Indeed, it remains a vital source of law within the present-day Nigerian legal system. It is true, as McDowell makes clear, that when the main body of English law initially came into force in Nigeria, the colonial authorities ostensibly anticipated that in due course, it "would be eroded and a new system would be created by local legislation and local decisions."[59] In reality, the

---

[54] *See* Bonny Ibhawoh, *Stronger Than the Maxim Gun Law, Human Rights and British Colonial Hegemony in Nigeria*, 72 AFR.: J. INT'L AFRICAN INST. 55, 59 (2002) (the pivotal role played by English law in the colonial subjugation of Nigeria has been well captured by this author who observes that "[the] process of consolidating and stabilising colonial rule was, of necessity, founded on law and specifically the English legal system . . . . Law, in the form of ordinances and proclamations . . . bec[a]me the basis of promoting British hegemony in the colony").

[55] Ordinance No.3 of 1873, § 1 (Nigeria).

[56] Supreme Court Ordinance, Ordinance No.6 of 1914. (Nigeria).

[57] *Id.* § 14.

[58] Watson, *supra* note 12, at 314.

[59] C. M. McDowell, *The Interpretation of the Land Tenure Law of Northern Nigeria,* 14 J. AFR. L. 155, 155 (1970). It was with this specific object in mind, that the reception formula in the Supreme Court Ordinance 1914, § 14, *supra* note 56, and similarly worded Nigerian statutory provisions enacted thereafter, (a) stipulated that the common law, Equity and English statutes of general application were subject to the terms of local ordinances and (b) provided a cut-off date of January 1, 1900 in respect to these statutes. *Id.*

colonial authorities made very little progress in this direction. On the contrary, as Sedler points out, "during the colonial period, the sad truth is that for the most part, English law as administered in Africa differed very little from the law administered in England."[60]

The lack of progress made by colonial authorities was symptomatic of the transplant bias and the inertia that permeated Nigeria's colonial and post-colonial legal systems.[61] As Watson explains, such transplant bias is present in situations where a legal system is inherently predisposed to foreign law emanating from a particular source.[62] Such bias encourages a high degree of acceptance by the recipient legal system, which is not necessarily based on a thorough examination of possible alternatives.[63] The extent of this bias depends on factors such as the existence of a shared linguistic tradition between the donor and recipient countries, the general prestige of the donor country, and the training and experiences of the legal profession in the recipient country.[64] Such bias is often compounded by inertia on the part of the regulatory elites which, according to Watson, is derived from the lack of a sufficiently strong impulse and the absence of any sustained interest in seeking out and giving effect to the most satisfactory or suitable rules.[65] Watson indicates that legal systems, which do not devote adequate legislative time or sufficient intellectual energy to the task of counteracting such inertia, tend to "tolerate much law which does not correspond to what is 'needed' or is efficient."[66] As Xanthaki points out, the clearest manifestation of such transplant bias in the legislative sphere is the fact that when faced with the prospect of drafting new legislation, drafting teams instinctively look to countries whose legal system, language, and tradition is familiar to their own

---

[60] Robert Allen Sedler, *Law Reform in the Emerging Nations of Subsaharan Africa: Social Change and the Development of the Modern Legal System*, 13 ST. LOUIS U.L.J. 195, 205 (1968–69).

[61] *See* L.E.O ESIEMOKHAI, THE COLONIAL LEGAL HERITAGE IN NIGERIA, 21–23 (1986) (arguing that the colonial government encouraged young Nigerians to go to England to study law intending that these future Nigerian lawyers would acquire the habits, tastes, and thought patterns of their British counterparts and that after Nigeria's independence, this articulate legal fraternity effectively ensured that there would be no sudden departure from British legal orthodoxy). *See also* Chukwuemeka G Nnona, *Towards the Decolonization of African Law*, *in* LAW, SECURITY AND DEVELOPMENT, COMMEMORATIVE ESSAYS OF THE UNIVERSITY OF NIGERIA LAW FACULTY 115, 142 (Chukwuemeka G Nnona ed., 2013) (explaining that the Nigerian legal system has displayed "an unquestioning disposition toward[s] received colonial constructs, especially a failure to seriously and comparatively interrogate the nature and history of the colonially-derived ideas and infrastructure of law.").

[62] Watson, *supra* note 12, at 327.

[63] *Id.*

[64] *Id.*

[65] *Id.* at 331.

[66] *Id.* at 332.

for guidance.[67] In the case of Nigeria, this meant that whenever the colonial legislative authorities set out to enact local ordinances intended either to supersede pre-1900 English statutes of general application, or to deal with matters not covered by such pre-1900 statutes, the contents of these local ordinances invariably bore a close affinity to corresponding statutes enacted by the U.K. Parliament after January 1, 1900.[68]

Gillespie remarks that in societies that have passed through the crucible of colonialism, it is "only after independence that a distance in legal perspective from the 'motherland' slowly begins to emerge."[69] This presupposes that the transplant bias exhibited by a legal system will start receding after it sheds the yoke of colonial bondage. In the case of Nigeria, however, even though more than fifty years have elapsed since it became an independent nation, it has so far done very little to distance itself from its Anglocentric legal antecedents and English law has continued to play a major role in many key spheres of human activity. The fundamental problem with the colonial transplant bias is that it is still deeply entrenched in Nigeria's postcolonial legal system, which has remained excessively deferential towards the received English law in its eagerness to preserve its Anglocentric legal traditions. Such deference sits uneasily with Nigeria's standing as an independent nation and is difficult to justify in an era when its political environment, social conditions, cultural milieu, and economic circumstances are very different from those that exist in British society.

Nigeria is by no means unique in this respect, as acknowledged by Sedler, who indicates that upon attaining independence, African states, "retained with little change the structure of the legal system that was 'inherited' from the colonial rulers."[70] Sedler suggests that this was understandable and perhaps even desirable since the indigenous legal elite entrusted with directing the development of these legal systems after independence "received their training in whatever law made up the essential elements of [their pre-]existing [colonial] system."[71]

---

[67] Xanthaki, *supra* note 11, at 660.

[68] Commenting on this state of affairs, Gower explains that

> [i]n general, local legislation was unimaginative – a verbatim reception of English law on the same subject matter. If, for example, a colony needed a Business Corporations Act, the Colonial Office would dispatch a copy of the latest English Companies Act [which in the case of Nigeria was the Companies (Consolidation) Act 1908, 8 Edw. 7, c 69 (Eng.)] and it would be re-enacted in the Colony without any consideration of whether it was really appropriate to local conditions.

L.C B GOWER, INDEPENDENT AFRICA: THE CHALLENGE TO THE LEGAL PROFESSION 27–28 (1967).

[69] GILLESPIE, *supra* note 9, at 4.

[70] Sedler, *supra* note 60, at 205.

[71] *Id*.

Gower on the other hand, has been rather less sanguine about the degree of prominence English law continued to enjoy in countries like Nigeria after independence. Gower points out rather acerbically that the legal elite in these countries viewed English law as "the perfection of human reason" and therefore deluded themselves that "everything in their legal garden [was] lovely."[72] In the face of such complacency, he maintained that he was not particularly proud of the legal legacy bequeathed by Britain to her African colonies because English law was often applied without consideration of its suitability to local conditions.[73] This has been the case in the Nigerian legislative arena where the excessively deferential attitude that has been displayed towards English law has led to the enactment of various statutes whose provisions are manifestly ill suited to local conditions and circumstances.

A notable example of a Nigerian statute that has adopted rules derived from English law without taking proper account of local circumstances is the Company and Allied Matters Act.[74] This Act provides that any association established for commercial purposes, which consists of more than twenty members, must be incorporated as a company. This means that under Nigerian law, unincorporated partnerships (other than cooperative societies and firms of legal practitioners or accountants) are prohibited from having more than twenty members.[75] Nnonna, who has undertaken an in-depth study of this particular provision,[76] explains that it can be traced back to the English

---

[72] GOWER, *supra* note 68, at 91.

[73] *Id.* at 30.

[74] Company and Allied Matters Act (1999), Chapter C20, Laws of the Federation of Nigeria 2010 (Nigeria).

[75] *Id.* § 19, which provides as follows:

> (1) No company, association or partnership consisting of more than twenty persons shall be formed for the purpose of carrying on any business for profit or gain by the company, association, or partnership, or by the individual members thereof, unless it is registered as a company under this Act . . . .
>
> (2) Nothing in this section shall apply to -
>
> (a) any cooperative society registered under the provisions of the any enactment in force in Nigeria; or
>
> (b) any partnership for the purpose of carrying on practice
>
> i. as legal practitioners, by persons each of whom is a legal practitioner; or
>
> ii. as accountants, by persons each of whom is entitled by law to practice as an accountant.

[76] C George Nnona, *The Prohibition of Large Partnerships in Nigerian Company Law: An Essay into Postcolonial Legal Atavism*, 11 SAN DIEGO INT'L L.J. 481, 483 (2010).

Companies Act 1948[77] and the English Companies Act 1967.[78] The wisdom of importing this particular rule of English law into Nigeria has been called into question by Nnona who argues that:

> Where two or more persons carry on business together with an expectation of profit, they are deemed to be a partnership. The sharing of profits from a joint enterprise is thus a prime indication of the existence of a partnership in law. The net result of this is that the provision . . . under consideration effectively renders illegal, myriad associations or arrangements under which people conduct sundry workaday activities . . . . A statutory provision should not proscribe myriad interactions that form part of the workaday life of the average citizen; not without a roundly considered and clearly articulated reason of an unassailable sort, something that is apparently lacking here. To do otherwise would be to implement legislation that is difficult to enforce [and] socially disruptive if enforced . . . ."[79]

It is evident from Nnona's analysis that this particular aspect of the received English law is not well suited to the sort of small-scale entrepreneurial activities that are very common in the Nigerian commercial environment. Indeed, the decision by Nigeria's legislative authorities to give effect to this arbitrary twenty-member limit is even more difficult to justify in view of the fact that this restriction no longer applies within the English legal system where it originated.[80]

Another statute that shows that Nigerian legislators are not yet adept at ensuring received English law is tailored to local conditions is the Nigerian Matrimonial Causes Act.[81] One of the remedies provided in this Act is a decree of jactitation of marriage.[82] This remedy is available to a petitioner against a respondent "who has falsely boasted and persistently asserted that a marriage has taken place between [them]."[83] The eminent legal historian, Richard Helmholz, indicates that suits for jactitation of marriage "began to be entertained by the English ecclesiastical courts from at least the late fifteenth

---

[77] Companies Act 1948, 11 & 12 Geo. 6, c 38, § 434 (Eng.).

[78] Companies Act 1967, c 81, § 120 (Eng.).

[79] Nnona, *supra* note 76, at 500–01.

[80] REGULATORY REFORM (REMOVAL OF 20 MEMBER LIMIT IN PARTNERSHIPS ETC) ORDER 2002, SI 2002/3203 (UK).

[81] Matrimonial Causes Act (1970), Chapter M7 Laws of the Federation of Nigeria 2010 (Nigeria).

[82] *Id.* § 2(2)(f).

[83] *Id.* § 52.

century forwards."[84] This remained the case until the enactment of the Matrimonial Causes Act 1857, which deprived the ecclesiastical courts of their jurisdiction in matrimonial matters (including jactitation of marriage) and transferred this jurisdiction to the newly created Court for Divorce and Matrimonial Causes.[85] With the passage of time, this remedy has become so obsolete that one notable scholar has described it as part of the "dead wood" of English matrimonial law and as a "near-fossil" whose passing "would be lamented by none."[86] As far back as 1971, the Law Commission of England and Wales expressed the view that "the remedy of jactitation of marriage is today inappropriate and should be abolished."[87] This recommendation was reiterated by the Law Commission in 1984[88] and was eventually implemented by the English Family Law Act 1986.[89] In spite of the fact that jactitation of marriage has been accorded legislative recognition in Nigeria, as it once was in England and in various other former British colonies, a perusal of the leading textbook on Nigerian family law reveals the remedy has merited only two very brief paragraphs. Moreover, there have been no known cases in which the remedy has been pursued in the Nigerian courts.[90] This suggests that this antiquated remedy is completely redundant in the Nigerian context and that its inclusion in the Nigerian Matrimonial Causes Act was unwarranted. This impression is reinforced by the fact that the remedy has been discarded in England where it originated and in various other jurisdictions where it once applied.

Even though many years have elapsed since the Nigerian Matrimonial Causes Act and the Company and Allied Matters Act were enacted, it seems that Nigeria's legislative authorities are still very much under the influence of the received English law. As shown in greater detail below, this is evident from the cavalier manner in which the current Nigerian National Assembly has sought to incorporate key provisions of the U.K. DPA into its draft legislation

---

[84] R. H. Helmholz, *Canonical Remedies in Medieval Marriage Law: The Contributions of Legal Practice*, 1 U. ST. THOMAS. L.J. 647, 654 (2003).

[85] Matrimonial Causes Act 1857, 20 & 21 Vict. c 85, § 2, § 6 (Eng.).

[86] H. A. Finlay, *Jactitation and Restitution of Conjugal Rights: An Epitaph*, 11 U.W. AUSTL. L. REV. 264 (1973–74).

[87] The Law Commission, *Published Working Paper No. 34: Jactitation of Marriage*, 8 (1971) (Eng.); *see also* ALBERTA LAW REFORM INSTITUTE, THE DOMESTIC RELATIONS ACT (DRA) PHASE 1, FAMILY RELATIONSHIPS: OBSOLETE ACTIONS 67–68, (1993) (arguing that actions for jactitation of marriage were "virtually unknown to Canadian jurisprudence," had "clearly outlived their usefulness" and should therefore be abolished in the Canadian province of Alberta).

[88] *See* The Law Commission, *Family Law: Declaration in Family Matters,* L.C No.132, paras. 4.1–4.11 (1984) (Eng.).

[89] Family Law Act, 1986, c 55, § 61 (Eng.). The remedy has also been abolished in other jurisdictions such as Australia and Ireland. *See Family Law Act*, *(1975),* (Cth) ch 53, § 8(2) (Austl.); Family Law Act, 1995, (Act No. 26/1995), § 34 (Ir.).

[90] *See* E.I. NWOGUGU, FAMILY LAW IN NIGERIA 250 (3d ed. 2014).

on data protection without undertaking any meaningful inquiry into their suitability to local conditions or the feasibility of seeking alternatives.

III. THE EMERGENCE OF DATA PROTECTION AS A SUBJECT OF LEGAL REGULATION IN NIGERIA

A. From Periphery to Center Stage: Nigeria's Place in Today's Global Information Society

Since the internet entered the public domain in the early 1990s, it has emerged as the main platform for the acquisition and exchange of information within the global arena. From the outset, internet usage was very heavily skewed in favor of the technologically advanced nations of the world. Commentators like Cullen refer to the emergence of a "digital divide" within the global community, which she attributed to the gap between the developed and underdeveloped world in the uptake of this new technology.[91]

Nigeria was a prime example of a country that, for many years, found itself on the wrong side of the digital divide. Until recently, there was surprisingly little online activity emanating from Nigeria despite the fact that it has one of the largest populations in the world, earns vast revenues as a major oil producer, and is Africa's largest economy.[92] Adomi, who has written extensively on the use of electronic information resources in Nigeria, reports that the web only became available in Nigeria in 1996 and that by the time full internet access was introduced in 1998, the nation had just a few dial-up email providers and a couple of internet service providers offering slow links to their subscribers.[93]

The Nigerian government was characteristically lethargic in its initial response to the onset of the internet revolution. It was not until 2001 that the government formulated a National Information Technology Policy and established the National Information Technology Development Agency ("NITDA") to implement this policy and coordinate the development of

---

[91] Rowena Cullen, *The Digital Divide: A Global and National Call to Action*, 21 ELECTRONIC LIBR. 247, 247 (2003), http://www.emeraldinsight.com/doi/pdfplus/10.1108/02640470310480506. *See also* Pippa Norris, *The Worldwide Digital Divide: Information Poverty, the Internet and Development*, Paper for the Ann. Meeting of the Pol. Stud. Ass'n of the UK (Apr. 12, 2000), http://www.hks.harvard.edu/fs/pnorris/Acrobat/psa2000dig.pdf (Norris stated that at the dawn of the new millennium, the (then) twenty-nine OECD nations which constituted the bulk of the world's post-industrial economies contained ninety-seven percent of all Internet hosts, ninety-two percent of the market in production and consumption of computer hardware, software and services, and eighty-six percent of all Internet users, while all of sub-Saharan Africa had just 2.5 million internet users).

[92] *See* LAUREN PLOCH BLANCHARD & TOMAS F HUSTED, CONG. RESEARCH SERV., NIGERIA: CURRENT ISSUES AND U.S POLICY, REPORT, 1 (2016), https://www.fas.org/sgp/crs/row/RL33964.pdf.

[93] Esharenana E. Adomi, *Internet Development and Connectivity in Nigeria*, 39 PROGRAM 257, 259 (2005), http://www.emeraldinsight.com/doi/pdfplus/10.1108/00330330510610591.

information technology in Nigeria.[94] Among the Agency's key objectives, as set out in the policy, were "[t]o promote legislation (Bills & Acts) for the protection of on-line,[*sic*] business transactions, privacy and security"[95] and "to enhance freedom and access to digital information at all levels while protecting privacy."[96] Although there was a gradual expansion in internet usage in the years after NITDA was established, it was estimated that by 2005 there were still fewer than five million internet users in Nigeria, which represented less than four percent of the population.[97] Adomi was therefore correct when he observed that Nigeria was "one of the slumbering giants of the African internet world."[98]

More recently, Nigeria's telecommunications sector has been revolutionized and liberalized by the introduction of the Global System of Mobile Communication ("GSM") technology needed to support the nation's new mobile telephone infrastructures.[99] Today, there are a number of mobile phone companies offering wireless access to the internet at competitive rates. In addition, a wide range of affordable internet-enabled smartphones, tablets, and other handheld digital devices have flooded the Nigerian market in recent years.[100] These developments have produced a massive surge in internet usage beginning in 2008 when there was an increase from just under ten million the previous year to nearly twenty-four million.[101] Since then, an ever-increasing number of Nigerians have become progressively more adept at navigating the digital environment. The Nigerian Communication Commission recently

---

[94] *See* FED. GOV'T OF NIGERIA, NIGERIAN NAT'L POL'Y ON INFO. TECH. (IT) (2001), http://www.researchictafrica.net/countries/nigeria/Nigerian_National_Policy_for_Information_Technology_2000.pdf [hereinafter POLICY ON INFO TECH].

[95] *Id.* at iv. (the legislative aspect of NITDA's mandate has subsequently been statutorily endorsed by the Nigerian National Information Technology Development Act (2007)); Chapter N156 Laws of the Federation of Nigeria 2010, § 6 (l) (Nigeria), http://www.nitda.gov.ng/wp-content/uploads/2016/02/NITDA-act-2007.pdf (providing that the Agency's functions include advising the Government "on ways of promoting the development of information technology in Nigeria including introducing appropriate information technology legislation")).

[96] *See* POLICY ON INFO TECH, *supra* note 94, at 32.

[97] *See* Internet Live Stats, *Nigerian Internet Users*, http://www.internetlivestats.com/internet-users/nigeria/.

[98] Adomi, *supra* note 93, at 257.

[99] *See* Esharenana E. Adomi, *Mobile Telephony in Nigeria*, 22 LIBR. HI TECH NEWS 18, 18 (2005), http://www.emeraldinsight.com/doi/pdfplus/10.1108/07419050510604648.

[100] *See e.g.* Adam Clayton Powell III, *Gallup/BBG Survey: 'Massive' Increase in Mobile Phone, Internet Use in Nigeria*, U. S.CAL Centre on Public Diplomacy Blog, Aug 16, 2012, http://uscpublicdiplomacy.org/blog/gallup_bbg_survey_massive_increase_in_mobile_phone_internet_use_in_nigeria.

[101] *See* Internet Live Stats, *supra* note 97.

announced that by September 2015 users browsing the Internet through Nigeria's GSM networks alone had exceeded ninety-seven million.[102]

B. The Law as a Mechanism for Safeguarding the Privacy of Personal Information: International, Regional and National Dimensions

Regulating the internet comes with a number of problems, as emphasized by Lim who argues that "[a]s was the case of previous technological revolutions throughout history, the law has been and will continue to be, stretched to its practical and theoretical limits in its efforts to overcome the challenges raised by the Internet."[103] The fact that society is now beset by the sort of challenges alluded to by Lim, clearly reveals that while the digital revolution undoubtedly has many positive aspects, it also has its less palatable dimensions. The double-edged nature of modern digital technology has been emphasized by the Global Commission on Internet Governance ("GCIG"), which explains that because the internet is "capable of communicating and storing almost unimaginable volumes of data online, including data that can be associated with each of us individually . . . [it] can be used for good or ill."[104] On the one hand, the advent of the internet and allied technologies has rendered it infinitely easier, considerably cheaper, and altogether more convenient for governmental, commercial, and voluntary organizations all over the world to accumulate, hold, and disseminate vast amounts of information for a variety of useful and legitimate purposes. On the other hand, many of these organizations have developed an almost insatiable appetite for personal information and have become adept at prying into the private affairs of individuals in their relentless quest for such information. The insidious nature of this phenomenon is reflected in the dystopian imagery employed by commentators, such as Murray, who speak of modern digital technology being deployed in an Orwellian fashion to monitor, manage and control the actions of the populace.[105]

The grim specter of modern information technology being exploited in such an intrusive manner has become a major conundrum within the legal arena

---

[102] *See NCC Says Nigeria Internet Users Rise to 97m*, METRO WATCH (Nigeria), http://metrowatchonline.com/ncc-says-nigeria-internet-users-rise-to-97m (last visited Oct. 1, 2016); *see also Nigeria: Mobile Internet Users Rise to 97.2 Mln,* IT NEWS AFRICA, http://www.itnewsafrica.com/2015/11/nigeria-mobile-internet-users-rise-to-97-2-mln/ (last visited Oct. 1, 2016).

[103] YEE FEN LIM, CYBERSPACE LAW: COMMENTARIES AND MATERIALS 1 (Trischa Baker ed., 2d ed. 2007).

[104] GLOBAL COMM'N ON INTERNET GOVERNANCE, TOWARD A SOCIAL COMPACT FOR DIGITAL PRIVACY AND SECURITY 3 (2015), https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150415GCIG2.pdf [hereinafter GCIG].

[105] Andrew D. Murray, *Should States Have a Right to Informational Privacy?, in* HUMAN RIGHTS IN THE DIGITAL AGE 191 (Andrew D. Murray & Mathias Klang eds., 2005).

with particular attention paid to the severe threat to individual privacy posed by the unfettered collection, inappropriate use, and indiscriminate transfer of personal information. The magnitude of the problem was highlighted at a fairly early stage by Lord Hoffman, the eminent U.K. Law Lord, who declared in the case of *R v. Brown* that:

> [O]ne of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual . . . . Vast amounts of information about everyone are stored on computers capable of transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is now under technological threat.[106]

Such concerns have not receded with the passage of time and the European Parliament recently pointed out that "[t]he growing globalization of data flows, via social networks, cloud computing, search engines, location-based services, etc., [has] increase[d] the risk that people can lose control of their own data."[107] The Nigerian population has become increasingly exposed to the sort of risk that has been highlighted by the European Parliament. This is because the use of search engines to navigate the internet is now very widespread in Nigeria,[108] numerous Nigerians have become avid and active social networkers,[109] and providers of cloud computing services are making steady inroads into the Nigerian market.[110]

Similar concerns have also been expressed by the GCIG, which emphasizes that trust in the internet is being eroded by the non-transparent manner vast amounts of private information is collected, centralized, integrated, and analyzed. GCIG maintains that in order to restore trust and enhance confidence, "fundamental human rights, including privacy and personal data protection, must be protected online" and "threats to these core human rights should be addressed by governments and other stakeholders acting both within their own jurisdictions and in cooperation."[111]

---

[106] R v. Brown [1996] AC 543 at 556 (Eng.).

[107] *EU Data Protection*, INTELLIGENCE IN SCI., www.iscintelligence.com/tema.php?id=13 (last visited Aug. 21, 2016).

[108] *See* Obiora Nwosu & Isaac Anyira, *The Use of Google and Yahoo by Internet Users in Nigeria*, LIBRARY PHILOSOPHY AND PRACTICE (E-JOURNAL) 10 (2012) http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1892&context=libphilprac.

[109] *See* AFRICA PRACTICE, THE SOCIAL MEDIA LANDSCAPE IN NIGERIA 4–6 (2014), http://www.africapractice.com/wp-content/uploads/2014/04/Africa-Practice-Social-Media-Landscape-Vol-1.pdf.

[110] *See* Gareth van Zyl, *Nigeria to Overtake SA to Become Africa's Cloud Computing Powerhouse*, ITWEBAFRICA (Nov. 14, 2013), http://www.itwebafrica.com/cloud/516-africa/231969-nigeria-to-overtake-sa-to-become-africas-cloud-computing-powerhouse.

[111] GCIG, *supra* note 104, at 1–2.

At the same time, however, even the most ardent privacy advocates have been pragmatic enough to appreciate the futility of trying to reverse the modern technological trends that precipitated the modern-day explosion of digital information. Instead, over the years, their efforts have largely been directed at deploying the law as an instrument for regulating rather than proscribing the processing of personal information. As Schartum remarks,

> Even though ICT may be used to reduce, even destroy, privacy, the same technologies almost always have a number of applications that lie well within the boundaries of what is regarded as acceptable - even from an information privacy point of view. Thus, information privacy and data protection are not expressions of a Luddite approach to technology, but rather about striking the right balance of interests by examining the boundary between acceptable and unacceptable use of ICT in different social contexts. This balance is formulated and implemented by means of regulation.[112]

Since the United States passed the Fair Credit Reporting Act in 1970, when computing was still in its infancy, numerous other nations have gone down the path of legal regulation of data processing by enacting legislation designed to protect personal information and safeguard the privacy of their citizens. Greenleaf, who in recent years has meticulously kept track of these nations, initially identified seventy-five nations in 2011.[113] Further inquiries undertaken revealed that the number had risen to 101 countries in September 2013[114] and 109 in 2015.[115]

At the same time, however, it is important to emphasize that because cyberspace is essentially a borderless environment, the regulation of data privacy has never been seen as the exclusive preserve of national governments. The global nature of the modern communication network has, in recent decades, resulted in a torrential flow of personal data across national boundaries.[116] The emergence of this global information network has

---

[112] Dag Wiese Schartum, *Designing and Formulating Data Protection Laws,* 18 INT'L J.L. & INFO. TECH. 1, 4 (2010).

[113] Graham Greenleaf, *Global Data Privacy in a Networked World, in* RESEARCH HANDBOOK ON GOVERNANCE OF THE INTERNET, 221, 224. (I. Brown, ed., 2012), papers.ssrn.com/sol3/papers.cfm?abstract_id=1954296.

[114] Graham Greenleaf, *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*, 23 J. L. INFO. & SCI. 4, 39 (2014).

[115] Graham Greenleaf, *Global Data Privacy Laws 2015: 109 Countries, with European Laws Now in a Minority*, 133 PRIVACY L. & BUS. INT'L REP. 1, 14–17 (2015).

[116] This trend was already clearly discernible as far back as 1983, when Yarn observed that,

> [T]he transfer of information across . . . boundaries is a phenomenon which predates written language. In today's world of satellites and computers, however, this flow of information has taken on added importance. The merger

inevitably meant that, in addition to the numerous national data privacy regimes that individual countries have introduced into their respective territories over the years, various international, regional, and sub-regional organizations have assumed a major role in shaping and defining how privacy is to be protected in the modern electronic age.

Commenting on this development, Kraus observes "[i]n the early 1980s there was an international movement for the intercontinental protection of personal data."[117] Greenleaf also remarks that "[i]nternational agreements concerning data protection have had a considerable influence on adoption of data privacy laws for thirty years."[118] The first notable step in this direction was taken in 1980, when the OECD produced a set of voluntary Guidelines Governing the Protection of Privacy and Transborder Flows.[119] A year later, the CoE went down the same route when it introduced its Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108).[120] Many of the member states of the CoE who ratified Convention 108 also happened to be members of the EU. One notable consequence of this is that the EU Data Protection Directive of 1995 (EU DPD),[121] which Greenleaf describes as the most influential international instrument on data privacy and which has served as the model for data protection legislation in many nations of the world, developed partly out of this Convention.[122]

> of previously disparate telecommunications and computer technologies has resulted in an "information technology" which reduces vast quantities of information to computer data, transferring it to points on earth and in space at remarkable speeds.

Douglas Yarn, *The Development of Canadian Law on Transborder Data Flows*, 13 GA. J. INT'L & COMP. L. 825, 825 (1983).

[117] Jennifer L. Kraus, *On the Regulation of Personal Data Flows in Europe and the United States*, COLUM. BUS. L. REV. 59, 67 (1993).

[118] Greenleaf, *supra* note 113, at 22.

[119] *See* Organization for Economic Co-operation & Development [OECD], *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, O.E.C.D. Doc. (C (80) 58 Final) (Oct. 1, 1980), *reprinted in* 20 I.L.M. 422 (1981). Although Nigeria is not an OECD member state, these Guidelines have had an indirect influence in the Nigerian setting. In particular, the ten privacy principles set out in PIPEDA, *supra* note 8, sch.1, are derived from these Guidelines and these ten principles have been reproduced virtually word for word in the Schedule to Nigeria's Personal Information and Data Protection Bill (2013), which will be examined in greater detail below.

[120] *See* Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Jan. 28, 1981, Eur. T.S. No. 108, *reprinted in* 20 I.L.M. 377 (1981).

[121] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard of Oct. 24, 1995 to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

[122] Greenleaf, *supra* note 113, at 22. Even though Nigeria is not an EU Member State and has never been under any treaty obligations to approximate its nascent data protection regime to this particular aspect of the EU's *acquis communautaire,* the indirect influence of the EU DPD within

With particular reference to African developments, the ECOWAS (of which Nigeria is a leading member) took the first tentative steps towards enacting its own sub-regional data privacy regime in October 2008 when ministers agreed on the text of what became the Supplementary Act on Data Protection within ECOWAS.[123] This supplementary Act was formally adopted by the Community's supreme organ, the authority of the heads of state and government in February 2010. Commenting on this instrument, Greenleaf indicates that it "establishes the content required of a data privacy law in each ECOWAS member state, including the composition of a data protection authority" and points out that all these requirements "are influenced very strongly by the EU Data Protection Directive."[124]

Under the ECOWAS Supplementary Act, each member state of the community is directed to "establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage, and use of personal data"[125] and to "establish its own [independent] data protection Authority . . . responsible for ensuring that personal data is processed in compliance with the provisions of this Supplementary Act."[126] In addition, the Supplementary Act elaborates on the composition, powers, and responsibilities of these data protection authorities[127] and sets out key principles guiding the processing of personal data.[128] The Supplementary Act also contains specific provisions relating to the processing of data, which under the EU data protection regime would be categorized as sensitive personal data.[129] The Supplementary Act also legislates against the transfer of personal data to non-ECOWAS member states that do not offer an adequate level of protection in relation to the processing of such data.[130] It also confers a number of rights on individuals whose personal data is being processed[131] and imposes various

---

the Nigerian legislative sphere is evident from the fact that this harmonizing Directive was implemented in the U.K. by means of the DPA 1998, *supra* note 7. Various key provisions of this U.K. statute have been incorporated almost verbatim into such draft Nigerian legislation as the Data Protection Bill 2011 and the Electronic Transactions (Establishment) Bill 2013, both of which will be considered further below.

[123] ECOWAS, Supplementary Act on Personal Data Protection within ECOWAS, Feb. 16, 2010, ECOWAS A/SA.1/01/10.

[124] GREENLEAF, *supra* note 113, at 26–27.

[125] ECOWAS, Supplementary Act on Personal Data Protection, art. 2.

[126] *Id.* at art. 14.

[127] *Id.* at arts.15–21.

[128] *Id.* at arts. 23–29.

[129] *Id.* at arts. 30–31.

[130] ECOWAS, Supplementary Act on Personal Data Protection, art 36.

[131] *Id.* at arts. 38–41.

obligations on personal data controllers engaged in the processing of such data.[132]

At the continental level, the African Union adopted a Convention on Cyber Security and Personal Data Protection in 2014.[133] This Convention sets out to strengthen the legislation relating to various aspects of digital technology in its Member States and to harmonize and co-ordinate their efforts at cyber-regulation.[134] Just as Greenleaf pointed out with reference to the ECOWAS regime, O'Donoghue indicates that many analysts believe that the data privacy regime embodied in Chapter II of the Convention "seeks to replicate the European Union data protection model whereby each country has its own national data protection laws and authority."[135] Greenleaf, for his part, regards the adoption of the Convention as the most notable global data protection development in 2014 and states that "[i]t is of great potential significance because the African Union has 54 member states, but its actual significance depends on accessions and ratifications, and as yet there are none."[136]

---

[132] *Id.* at arts. 42–45.

[133] Afr. Union, *African Union Convention on Cyber Security and Personal Data Protection,* EX.CL/846(XXV), (June 27, 2014).

[134] *See* Afr. Union, *Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa,* http://www.au.int/en/cyberlegislation ("The Draft Convention . . . seeks to harmonize African cyber legislations [*sic*] on electronic commerce organization, personal data protection, cyber security promotion and cyber crime control [and] . . . also to strengthen existing legislations [*sic*] in Member States and the Regional Economic Communities (RECs) on the Information and Communication Technologies.") (last visited Oct 1, 2016).

[135] Cynthia O'Donoghue, *New Data Protection Laws in Africa,* TECHNOLOGY LAW DISPATCH (Feb. 19, 2015), http://www.technologylawdispatch.com/2015/02/regulatory/new-data-protection-laws-in-africa/. This is particularly evident from art. 8 (which commits each Member State to establishing a legal framework aimed at strengthening the protection of personal data and preventing violations of privacy arising from the collection, processing, transmission and storage of such data); and arts. 11–12 (which require member states to establish their own independent national personal data protection authorities and specify the duties and powers of these authorities). Other notable elements of the Convention's data protection are: (a) the set of basic principles governing the processing of personal data (art. 13); (b) the more specific principles governing the processing of sensitive personal data (art. 14); (c) the restrictions imposed on the transfer of personal data to non-African Union member states that do not ensure an adequate level of protection (art. 14(6)); (d) the rights conferred on data subjects (arts. 16–19) and (e) the obligations imposed on personal data controllers (arts. 20–23); *see also* Makulilo, *supra* note 29, at 81–82 (explaining the key features of the Convention).

[136] Greenleaf, *supra* note 114, at 5.

IV. NIGERIA'S LEGISLATIVE ENGAGEMENT WITH THE DATA PRIVACY AGENDA: A CATALOGUE OF FALSE STARTS AND DEAD ENDS

A. Overview

Kusamotu observed in 2007 that "[t]he Nigerian economy and technology are both on the up-surge, but as yet are at levels that do not lead to a significant awareness of privacy issues in data processing," and noted in particular that "there ha[d] not been any significant ground-swell clamoring for EU-style data protection law in Nigeria."[137] Despite the fact that Nigeria has experienced exponential increases in internet usage and is now awash with PCs, laptops, and other internet-enabled devices, it still has not joined the swelling ranks of the world's countries that have enacted their own data privacy laws.[138] In Africa alone there were, at the last count, seventeen such countries[139] and Nigeria's conspicuous absence from the fold has been commented upon by Makulilo who points out that "[a]s most of the countries which have so far adopted data protection are relatively weak economically and politically, the spotlight will increasingly be put on Nigeria as one of the most economically and politically significant countries in Africa still without a data protection law."[140]

The fact that there has not yet been any discernible urgency on the part of the Nigerian government to enact its own data privacy regime is highly surprising for several reasons. First, constitutional democracy has at last taken root in Nigeria, and the right to privacy happens to be one of the fundamental rights enshrined in Nigeria's current Constitution.[141] Even though there is no specific right to the protection of personal data of the type provided for in the EU Charter of Fundamental Rights,[142] the broader formulation in section 37 of the Constitution clearly encompasses this right.

---

[137] Ayo Kusamotu, *Privacy Law and Technology in Nigeria: The Legal Framework will not Meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/46*, 16 INFO. & COMM. TECH. L. 149, 156 (2007).

[138] *See* Peter C. Obutte, *ICT Laws in Nigeria: Planning and Regulating a Societal Journey into the Future*, 17 POTCHEFSTROOM ELECTRONIC L.J. 419, 438 (2014) ("[t]he huge possibilities and benefits that accompany ICT deployment have been obscured by an indifference to appropriate regulation on privacy. ICT in Nigeria is developing without a legal framework to protect the privacy of individuals in this rapidly evolving ICT environment.").

[139] *See* Greenleaf, *supra* note 114, at 3.

[140] Makulilo, *supra* note 4, at 25.

[141] Constitution of the Federal Republic of Nigeria (1999) § 37 (Nigeria) ("The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."). For a more detailed analysis of this constitutional right, see E.S Nwuche, *The Right to Privacy in Nigeria*, 1 CENTER FOR AFR. LEGAL STUD. REV. OF NIG. L. & PRACT. 83–89 (2006).

[142] The Charter of Fundamental Rights of the European Union art. 8(1), Dec. 7, 2000, 2000 O.J. (C 364) 1 ("Everyone has the right to the protection of personal data concerning him or her.").

Secondly, as Makulilo points out, by virtue of Nigeria's membership of ECOWAS, "it has an obligation to adopt a data protection law in conformity with the ECOWAS Supplementary Act . . . ."[143] This is because Article 9(4) of the Revised ECOWAS Treaty stipulates that a decision of the authority of the heads of state and government "shall be binding on the member states and institutions of the Community."[144] The binding effect of such decisions is reflected in Articles 47 and 48 of the Supplementary Act, which deal with the publication and entry into force of the Supplementary Act. Article 47 stipulates that,

> This Supplementary Act shall be published by the Commission in the Official Journal of the Community within thirty (30) days of signature by the Authority of Heads of State and Government. It shall equally be published by each Member State in its national Gazette thirty (30) days after notification by the Commission.[145]

Article 48 goes on to provide that "this Supplementary Act shall enter into force upon publication in the Official Journal of the Community and in the Official Gazette of each Member State."[146] Because the Supplementary Act was signed by the Authority of Heads of State and Government on February 16, 2010, the procedure prescribed in Articles 47 and 48 meant that it should have been published by the Commission in the Official Journal of the Community by March 18, 2010, and by each Member State in its Official Gazette by April 17, 2010, at which point it should have entered into force. It might have been expected, in the light of these provisions that all ECOWAS Member States, including Nigeria, would have proceeded without undue delay either to enact national data protection laws modeled on the Supplementary Act or to recast any data protection laws they might already have enacted to bring them into line with the new ECOWAS regime. It is somewhat ironic that the very meeting at which the heads of state endorsed this instrument took place in the Nigerian capital, Abuja, and was presided over by the nation's then acting president, Goodluck Jonathan, who was also one of the signatories. Nigeria might therefore have been expected to be in the vanguard of West African nations seeking to give effect to this instrument through their domestic legislative processes.

Thirdly, Makulilo emphasizes that "a powerful driver of the development of privacy law among developing countries is the desire to engage in global e-Commerce" and that "undoubtedly this has been the paramount motivation for

---

[143] Makulilo, *supra* note 4, at 25.

[144] Revised Treaty of the Economic Community of West African States (July 24, 1993), art. 9(4), 35 I.L.M. 660, 669 (1996).

[145] ECOWAS, Supplementary Act on Personal Data Protection, art. 47.

[146] *Id.* at art. 48.

the adoption of data privacy legislation in Africa."[147] In the case of Nigeria, as Ambassador Michel Arrion, the Head of the EU Delegation to Nigeria, recently pointed out, the EU is the nation's most important trade partner and its biggest market for both oil and non-oil exports.[148] EU trading operations have increasingly begun to use electronic processes, which often entail the transfer of personal data to destinations outside the EU. The EU DPD permits such transfers to a non-EU Member State only where it ensures an adequate level of protection or where adequate privacy safeguards are imposed on the non-EU recipient of the data (e.g. by means of appropriately worded contractual provisions or binding corporate rules).[149]

In order to ensure that its trading arrangements with various EU Member States are not hindered unduly by these adequacy requirements, Nigeria might have been expected to treat the issue of data protection as a matter of legislative priority.

This expectation has become more intense because other major sub-Saharan economies like Ghana and South Africa, which are in fierce competition with Nigeria to make inroads into the highly lucrative EU markets, have now enacted their own well drafted and fairly comprehensive data protection statutes.[150] Nigeria, by contrast, has been very slow to legislate for data privacy, prompting some authors to assert that

> [a]s a developing economy that is eager to be placed on the same map with the economically advanced nations of the world, the realities on [the] ground mandate that . . . Nigeria should have adequate legislation to protect information especially in the terrain of electronic commercial transactions. Till date, Nigeria does not have any data protection legislation that is comparable to that in operation in other countries . . . . As a matter of fact, there is no federal or state enactment of

---

[147] Makulilo, *supra* note 29, at 79.

[148] *See* Hakeem Jimo, Speech Delivered by Ambassador Michel Arrion at the EU-Nigeria Business Forum (Sep. 23, 2014) (transcript available at http://www.thenigerianvoice.com/lifestyle/158022/speech-delivered-by-ambassador-michel-arrion-at-the-eu-niger.html).

[149] EU DPD, arts. 25–26.

[150] Protection of Personal Information Act (Act No. 4/2013) (S.Afr.), http://www.justice.gov.za/legislation/acts/2013-004.pdf; *see* Pamela Stein, *South Africa Adopts Comprehensive Privacy Law*, 126 PRIVACY L. & BUS. INT'L REP. 1, 3–4 (2013); Mark J. Calaguas, *South African Parliament Enacts Comprehensive Data Protection Law: An Overview of the Protection of Personal Information Bill*, AFR. L. TODAY (2013), http://works.bepress.com/mark_calaguas/15/ (both of which examine the scope and highlight key aspects of the South African legislation); *see also* Data Protection Act (Act No. 843/2012) (Ghana), https://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843.

> legislation that has the protection of personal data as its main object within the Nigerian legislative framework.[151]

Nigeria's legislative efforts have only spawned a motley assortment of poorly conceived, inexpertly drafted, and far from comprehensive bills that are ill-attuned to emerging trends, rapid changes, and regulatory complexities inherent in data protection. This Article examines these bills in roughly chronological order to substantiate this admittedly harsh assessment of Nigeria's legislative attempts.

B. The Cyber Security and Data Protection Agency Bill 2008

The Cyber Security and Data Protection Bill represents one of the Nigerian Legislature's earliest attempts to regulate the online activities of its citizenry. One of the bill's primary aims was to establish the Cyber Security and Information Protection Agency.[152] To satisfy the ECOWAS Supplementary Act and the African Union Convention, any data protection regime enacted for Nigeria must be administered by an independent data protection authority.[153] A perusal of the Bill, however, reveals that the members of the Cyber Security and Information Protection Agency were mainly government functionaries, making the Agency far from an independent authority.[154] Furthermore the key functions of the Agency, as prescribed by the Bill, bear no relationship to the type of matters that ordinarily fall within the remit of most data protection authorities.[155]

When this bill is read in its entirety, it is evident that it was not intended to be the harbinger of a new data protection regime in Nigeria. Instead, the bill prescribes a wide range of criminal offenses relating to the misuse of computers,[156] imposes certain duties on internet and communication service providers,[157] and empowers the Nigerian president to designate certain computer systems and communication networks as part of the nation's critical information structure.[158] The inclusion of the phrases "Data Protection" in the

---

[151] Jemilohun & Akomolede, *supra* note 4, at 1–2.

[152] Cyber Security and Data Protection Agency Bill, H.B. 154 (2008) § 1(1) (Nigeria).

[153] *See* ECOWAS Supplementary Act, on Personal Data Protection, art. 14; *African Union Convention on Cyber Security and Personal Data Protection*, *supra* note 133, at arts. 11–12.

[154] *See* Cyber Security and Data Protection Agency Bill, H.B. 154 (2008) § 2 (Nigeria).

[155] *Id.* § 4.

[156] *Id.* §§ 7–8 (unlawful access to computers and unauthorized disclosure of computer passwords and access codes); §§ 9–10 (fraudulent electronic messages and other forms of computer fraud); §§ 11–12 (interference with computer networks and misuse of electronic devices); §§ 19–20 (cybersquatting and other computer-based violations of intellectual property rights); § 20 (cyberterrorism); § 22 (cybergrooming and child pornography).

[157] *Id.* §§ 15, 17.

[158] Cyber Security and Data Protection Agency Bill, H.B. 154 (2008) § 24 (Nigeria).

title of the bill and "Information Protection" in the name of the agency is thus utterly redundant and wholly misleading.

C. The Data Protection Bill 2011

The substantive provisions of this Bill are closely based on the U.K. DPA 1998.[159] In *R (On the application of Catt) v Commissioner of Police of the Metropolis and another,* Lord Sumption recently described the DPA 1998 as a statute of general application.[160] As seen above, the statutory formula for the reception of English law into Nigeria provided that "the common law, the doctrines of equity and the statutes of general application which were in force in England on the first of January 1900 shall be in force [in Nigeria]."[161] This suggests that if the legal problems the DPA 1998 seeks to address had existed in the nineteenth century and if the DPA had been enacted before the first of January 1900, it would have been one of the acts of the U.K. Parliament received by Nigeria alongside the common law and principles of equity.

The Data Protection Bill 2011 ("the Bill") consists of just eleven sections, with section 10 being the definition section and section eleven merely setting out its short title. The DPA 1998, by contrast, consists of seventy-five sections and sixteen lengthy schedules.[162] This marked disparity reflects the fact that the Bill merely scratches the surface, is highly selective in its coverage, and does not do justice to the complexity, technicality and constantly evolving nature of the modern data privacy agenda.

Section 1 of the Bill sets out the principles governing the handling of personal data.[163] These principles are virtually identical to the eight data protection principles contained in the DPA 1998.[164] However, the Bill does not provide the type of guidance on the interpretation of these principles that is contained in the DPA 1998.[165] Moreover, under the bill, the all-important principle that data must be processed "fairly and lawfully"[166] is not underpinned by any provisions of the type that are found in Schedules 2 and 3 of the DPA 1998 concerning the procurement of the data subject's consent or any of the other alternative conditions that must be present for data to be adjudged to have been lawfully processed.

---

[159] Data Protection Bill, H.B. 45 (2011) (Nigeria); Data Protection Act, 1998, c 29 (Eng.).

[160] R v. Comm'r. of Police of the Metro. [2015] UKSC 9, para. 12 (Eng.).

[161] *See* Supreme Court Ordinance, Ordinance No.6 of 1914, § 19 (Nigeria).

[162] Data Protection Act, 1998, c 29 (Eng.).

[163] Data Protection Bill, H.B. 45 (2011), § 1 (Nigeria).

[164] Data Protection Act, 1998, c 29, sched.1 Part I (Eng.).

[165] *Id.* at sched.1, Part II.

[166] Data Protection Act, 1998, c 29, scheds. 2 & 3 (Eng.).

Other key provisions of the Bill confer a variety of rights on the data subject. These include the right of access to any personal data relating to the data subject that is being processed by or on behalf of a data controller,[167] the right to require data controllers to cease to process such personal data,[168] the right to prevent the data controller from exploiting such data for direct marketing purposes,[169] the right to require data controllers to ensure that no decision taken by them which significantly affects the data subject is based solely on the processing by automatic means of such data,[170] and the right to require data controllers to rectify, block, erase or destroy such data in certain circumstances.[171] Additionally, the Bill confers on data subjects a right to compensation from the data controller for any damage arising from any contravention of their data processing obligations.[172] These rights have been formulated in precisely the same terms in the Bill as their corresponding rights in the DPA 1998.[173]

Makulilo has drawn attention to significant deficiencies in this piece of legislation, particularly when it is compared to the U.K. DPA.[174] He points out, for instance, that unlike the DPA 1998, it is not entirely clear whether the Bill is intended to regulate the public sector, the private sector, or both.[175] He also indicates that even though the Bill, elaborates on what constitutes "sensitive personal data,"[176] the Bill does not contain any of the extra safeguards surrounding the processing of such data that have been provided for in the U.K. DPA.[177]

In addition, Makulilo notes that while the Bill, like its U.K. counterpart, seeks to preclude the transfer of personal data from Nigeria to other countries that do not ensure an adequate level of protection,[178] the Bill does not stipulate

---

[167] Data Protection Bill, H.B. 45 (2011), § 2 (Nigeria).

[168] *Id.* § 3.

[169] *Id.* § 4.

[170] *Id.* § 5.

[171] *Id.* § 7.

[172] Data Protection Bill, H.B. 45 (2011), § 6 (Nigeria).

[173] *See* Data Protection Act, 1998, c 29 (Eng.) (where the corresponding sections are: § 8 (right of access); § 10 (right to require data controller to cease processing); § 11 (right to prevent processing for direct marketing purposes); § 12 (right in relation to automatic decision taking); § 14 (right to rectification etc.) and; § 13 (right to compensation)).

[174] Makulilo, *supra* note 4, at 25–27.

[175] *Id.* at 25.

[176] *See* Data Protection Bill, H.B. 45 (2011), § 10 (Nigeria); Data Protection Act, 1998, c 29, § 2 (Eng.).

[177] Makulilo, *supra* note 4, at 26.

[178] *See* Data Protection Bill, H.B. 45 (2011), § 1(4) (Nigeria); Data Protection Act, 1998, c 29, sched. 1 (Eng.) (the eight data protection principles).

who should carry out the "adequacy" assessment, how this should be done, and according to which criteria,[179] even though these matters were addressed at some length by the DPA 1998.[180] Makulilo also points out that most national data protection statutes (including the UK DPA) contain exemptions respecting processing of personal data for a variety of public interest purposes, like national security, law enforcement, and journalistic integrity,[181] but there are no such exemptions in the 2011 Bill.[182]

Most importantly, Makulilo highlights the fact that in marked contrast to the DPA 1998, and most other data privacy legislation around the world, the Bill contains no provision for a data protection authority or commission to oversee its operation.[183] He makes the valid point that this omission "weakens the Nigerian Bill significantly to the extent of falling short of international standards."[184] Makulilo is entirely correct when he concludes that "[i]n its present formulation, Nigeria's Data Protection Bill presents a weak standard of legislation in comparison to other jurisdictions in Africa and beyond."[185] The various inadequacies in the Bill are further compounded by its lack of recognition of various other key aspects of the DPA 1998, including the registration and notification requirements set out in Part III, the enforcement mechanisms provided in Part V, or the criminal offenses and monetary penalties specified in Part VI. All in all, the 2011 Bill is an amateurish piece of draft legislation that poorly reflects the principal legislative organ of one of Africa's leading nations.

D. The Electronic Transactions (Establishment) Bill 2013

The very obvious shortcomings of the Data Protection Bill 2011 clearly suggest that it was drafted without due care or a proper understanding of the U.K. data protection regime on which the Bill was modeled. Having produced such a woefully unsatisfactory Bill at their first attempt, the Nigerian National Assembly should have devoted a great deal more time and effort to devising a more comprehensive piece of legislation that would not just outline the basic duties imposed on data controllers by the data protection principles and the accompanying rights conferred on data subjects, but also provide the administrative machinery and enforcement processes that would underpin the operation of the legislation. This has, however, proved to be something of a

---

[179] Makulilo, *supra* note 4, at 26.

[180] *See* Data Protection Act, 1998, c 29, scheds. 1, 4 (Eng.).

[181] *Id.* § 28 (national security exemption); § 29 (law enforcement exemption); § 32 (exemption relating to journalistic, literary, and artistic materials).

[182] Makulilo, *supra* note 4, at 26.

[183] *Id.*

[184] *Id.*

[185] *Id.* at 27.

forlorn hope since the Electronic Transactions Bill 2013 does not represent much of an improvement on the Data Protection Bill 2011.

The 2013 Bill is more compendious in scope than the 2011 Bill. The 2013 Bill covers not only data protection, but also a variety of other contemporary legal issues pertaining to electronic communications such as the effect of the requirements of writing and signature on electronic documents, principles governing the formation of electronic contracts, and consumer protection issues.[186]

The arrangement of sections that precedes the main body of the 2013 Bill indicates that Part IV, which deals with data protection, consists of sections 19 to 27,[187] whereas in the main body of the bill itself, Part IV actually consists of sections 17 to 25.[188] The presence of such an egregious error in a draft Bill laid before Nigeria's highest legislative body is utterly indefensible and calls into question the lack of attention to detail and the caliber of the legislative drafters working for the National Assembly. Of even greater concern is the fact that in attempting to shoehorn such a broad and diverse spectrum of matters into a single legislative instrument, the drafters of the 2013 Bill devoted a meager nine sections to their legal and regulatory scheme for the protection of personal data.[189] This is inadequate and absurd, given the complex, convoluted and rapidly evolving nature of this area of law. It would have been preferable if the drafters had devoted resources to producing a separate bill specifically designed to regulate the sphere of data protection in a meticulous, comprehensive, and meaningful manner.

Instead, Part IV of the 2013 Bill (like the 2011 Bill) is primarily concerned with outlining the data protection principles that data controllers (or data holders as they are referred to here) must observe[190] and specifying the rights

---

[186] Electronic Transactions Bill, S.B 248 (2013), § 1 (Nigeria). The relevant section provides:

> This Bill is to provide a legal and regulatory framework for:
>
> (a) conducting transactions using electronic or related media;
>
> (b) the protection of the rights of consumers and other parties in electronic transactions and services;
>
> (c) the protection of personal data; and
>
> (d) facilitating electronic commerce in Nigeria.

[187] *Id.*

[188] *Id.* Part IV, §§ 17–25.

[189] *Id.* §§ 17–25.

[190] *Id.* § 18 (1) (conditions for the processing of personal data); § 18 (2)–(7) (other data protection principles that data holders must comply with); § 19 (conditions for the processing of sensitive personal data by data holders); §§ 23–24 (obligation of data holder to ensure that appropriate technical and organizational requirements are in place to protect personal data).

exercisable by data subjects (referred to in this context as data owners).[191] Of particular interest is the fact that the second, third, fourth, fifth, sixth, and eighth data protection principles outlined in Schedule 1 of the DPA 1998 have been re-enacted virtually word-for-word in the 2013 Bill.[192] Moreover, a variant of the seventh data protection principle is provided for elsewhere in the 2013 Bill.[193] It is somewhat surprising that having provided for seven of the eight data protection principles set out in the DPA 1998, the relevant sections of the 2013 Bill make no specific reference to the requirement that data must be processed fairly and lawfully, which forms the basis of the first data protection principle.[194] Schedule 1(1) of the DPA 1998 provides that in order for personal data to be processed fairly and lawfully, at least one of the conditions set out in Schedule 2 must be met.[195] All these conditions have been reproduced almost *verbatim* in the 2013 Bill.[196] Therefore it is rather perplexing that there is

---

[191] Electronic Transactions Bill, S.B 248 (2013), § 20 (Nigeria).

[192] *Id.* § 18(2)–(7). The relevant subsections of the Bill provide as follows:

> (2) Personal data shall be obtained only for specified and lawful purposes, and shall not be further processed in any manner incompatible with those purposes.
>
> (3) Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.
>
> (4) Personal data shall be provided accurately and, where necessary, kept up to date.
>
> (5) Personal data processed for whatever purpose, shall not be kept for longer than required.
>
> (6) Personal data shall be processed in accordance with the rights of data owners under the laws of the Federal Republic of Nigeria.
>
> (7) Personal data shall not be transferred to a country or territory outside the Federal Republic of Nigeria unless that country or territory provides adequate level of protection for the rights and freedoms of data owners in relation to the processing of personal data.

[193] *Id* § 23(1) ("A data holder must implement appropriate technical and organizational measures and exercise reasonable care to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, processing, disclosure or access . . . and against all other unlawful forms of processing.").

[194] *Id.* §§ 18, 23.

[195] *See* Data Protection Act, 1998, c 29, sched. 1(1) (a) (Eng.).

[196] Electronic Transactions Bill, S.B 248 § 18(1) (Nigeria). This subsection provides as follows:

> Personal data shall only be processed if at least one of the following conditions met:
>
> (a)The data owner has given his consent to the processing.
>
> (b) The processing is necessary for the performance of a contract to which the data owner is a party, or for the taking of steps at the request of the data owner with a view to entering into a contract.

nothing whatsoever in the 2013 Bill linking these conditions to the requirement in the first data protection principle that data must be fairly and lawfully processed.

One material difference between the 2011 Bill and the 2013 Bill is that the 2013 Bill (like the DPA 1998) identifies a number of contexts in which processing of personal data is exempt from the strict requirements of the legislation. Such exemptions include processing that occurs in the realms of public safety, defense, national security, law enforcement, crime prevention, and protection or where processing is undertaken by natural persons in the course of their personal or domestic activities.[197] At the same time, however, there are certain other important exemptions contained in the DPA 1998 that do not appear in the 2013 Bill.[198] It is also noteworthy that sections of the 2013 Bill, which set out the rights exercisable by data subjects,[199] have inexplicably omitted three of the rights specified in the DPA 1998 as well as the 2011 Bill. These are the right to prevent data controllers from exploiting personal data for direct marketing purposes,[200] the right to require data controllers to ensure that no decision taken by them which significantly affects the data subject is based solely on the processing by automatic means of personal data,[201] and the

---

> (c) The processing is necessary for compliance with any legal obligation to which the data holder is subject, other than an obligation imposed by contract. [sic]
>
> (d) The processing is necessary in order to protect the vital interests of the data owner.
>
> (e) The processing is necessary in the interest of the public and good governance.

[197] *Id.* § 17(2). The relevant subsection of the Bill provides that the subsections of the Bill "shall not apply to the processing of personal data:

> (a) in the course of an activity concerning public safety, defence [or] national security;
>
> (b) concern[ing] the activities of law enforcement, intelligence or prosecuting agencies in areas of criminal law;
>
> (c) by a natural person in the course of personal or domestic activity." *Id.* The U.K. DPA contains analogous provisions. Data Protection Act, 1998, c 29, §§ 28, 29, 36 (Eng.) (referring to national security, crime prevention and detection, and domestic purposes).

[198] Exemptions that are not covered by the Electronic Transactions Bill 2013, even though they are provided for in the DPA 1998, include exemptions relating to the processing of personal data for journalistic, literary, or artistic purposes (§ 32) or research purposes (§ 33); the processing of personal data in circumstances covered by parliamentary privilege (§ 35A) as well as various miscellaneous exemptions set out in sched. 7 (§ 37).

[199] Electronic Transactions Bill, S.B 248 (2013), §§ 20–23 (Nigeria).

[200] Data Protection Act, 1998, c 29, § 11 (Eng.); Data Protection Bill, H.B. 45 (2011), § 4 (Nigeria).

[201] *See* Data Protection Act, 1998, c 29, § 12 (Eng.); Data Protection Bill, H.B. 45 (2011), § 5 (Nigeria).

right to require data controllers to rectify, block, erase, or destroy personal data in certain circumstances.[202]

Finally, the 2013 Bill provides that the Nigerian National Information Technology Development Agency ("NITDA") "may in consultation with any appropriate regulatory body, develop rules and guidelines for Data Protection in Nigeria."[203] This is consonant with powers conferred on NITDA by the National Information Technology Development Agency Act 2007, which provides in this connection that NITDA will play a key role in advising "on ways of promoting the development of information technology in Nigeria including introducing appropriate information technology legislation."[204] NITDA has accordingly prepared several sets of draft Guidelines on Data Protection, the most recent being Version 4.0, which was produced in September 2013.[205] It is not entirely clear what the precise legal status of the NITDA Guidelines will be if, and when, they are eventually enacted. In any case, the NITDA Guidelines add very little of significance to the provisions of the 2013 Bill, other than requiring any organization engaged in the processing of personal data: (1) to implement effective privacy policies and procedures and publish such policies publicly;[206] (2) to undertake detailed benchmark assessments of such policies;[207] and (3) to designate an employee as its Data Security Officer to be responsible for adherence to these data protection policies and procedures and for effective data protection and management within the organization.[208]

The NITDA Guidelines have also taken steps towards plugging a gap in the 2013 Bill by setting out some criteria for determining whether countries outside Nigeria provide an adequate level of protection for data export purposes.[209] However, it is noteworthy that the NITDA Guidelines do not dispense with the need for the recipient country to ensure an adequate level of protection where alternative mechanisms for safeguarding data exports (such as the binding corporate rules and model contractual clauses) are put in place. This could easily have been done by including in the Guidelines, provisions

---

[202] *See* Data Protection Act, 1998, c 29, § 14 (Eng.); Data Protection Bill, H.B. 45 (2011), § 7 (Nigeria).

[203] Electronic Transactions Bill, S.B 248 (2013), § 25 (Nigeria).

[204] *See* Nigerian National Information Technology Development Act, Chapter N156 Laws of the Federation of Nigeria 2010 (Nigeria)) § 6(1).

[205] NAT'L INFO. TECH. DEV. AGENCY, GUIDELINES ON DATA PROTECTION VERSION 4.0 (2013), nitademo.azurewebsite.net/wp-content/uploads/2016/06/Guidelines-On-Data-Protection-Final-Draft-3.4.Pdf [hereinafter NITDA Guidelines].

[206] *Id.* § 2.1.6.

[207] *Id.* § 3.1.2.

[208] *Id.* § 3.1.1.

[209] *Id.* §§ 2.2.5–7.

along the lines of Article 26(2) of the EU DPD[210] or Schedule 4 (8) and (9) of the DPA 1998.[211] It is true that the NITDA Guidelines provide that if a requirement exists to send or transfer data outside Nigeria, data controllers should consider whether the data is "being processed outside of the [sic] Nigeria by another office of the same firm which is established within Nigeria," and should also consider whether there is "a contract in place between the data controller and the receiving organization providing for adequate protection of personal data."[212] Significantly, the NITDA Guidelines do not go on to stipulate that the need for the recipient country to ensure an adequate level of protection will be relaxed in circumstances where the Nigerian office and the office outside Nigeria, to which the data is being exported, are both subject to adequate uniform corporate rules pertaining to the protection of personal data or where the contract in question confers an adequate degree of protection on the data that is being exported.

Although the 2013 Bill includes several features one might expect in a modern data protection regime, as opposed to the 2011 Bill (especially when read in conjunction with the draft NITDA Guidelines), it is still no more than a pale imitation of the DPA 1998. The 2013 Bill does not go very far towards remedying the defects in the 2011 Bill and, in particular, makes no provision for the establishment of a data protection authority. Further, the 2013 Bill ignores the numerous proposals for reforming the EU DPD contained in the EU GDPR. [213]

These proposed reforms, which are to be implemented in May 2018, will have a significant impact on the current state of data protection law throughout the EU, both from the standpoints of the data subject and the data controller. On the one hand, the rights of data subjects will be strengthened by measures like: (a) the introduction of a significantly higher threshold for proving data subjects have consented to the processing of their personal data,[214] (b) the conferment of a "right to be forgotten" on data subjects when they no longer want their personal data to be processed and there is not legitimate need to retain said data,[215] and (c) the conferment of a "right of data portability" which will entitle data subjects whose personal data has been processed by electronic means to transfer such data into another electronic processing system without hindrance from the data controller.[216]

---

[210] EU DPD, art. 26(2).

[211] Data Protection Act, 1998, c 29, sched. 4(8)–(9) (Eng.).

[212] *See* Nigerian National Information Technology Development Act (2007) Cap. (N156), § 4.1.8.

[213] *See* EU GDPR, Regulation 2016/679, *supra* note 1.

[214] *Id.* at art. 4(11).

[215] *Id.* at art. 17.

[216] *Id.* at art. 20.

In addition to strengthening the rights of data subjects, the regulation will also increase the levels of responsibility and accountability demanded from data controllers. Specifically, this regulation will require data controllers to: (a) notify the relevant data protection authorities and data subjects of serious data breaches,[217] (b) carry out data protection impact assessments when engaged in processing operations that present specific risks,[218] (c) appoint specialist data protection officers in certain circumstances such as where the data controller is a public authority,[219] (d) implement appropriate technical and organizational measures and procedures and integrate safeguards into processing designed to protect the rights of data subjects (privacy by design),[220] and (e) ensure privacy-friendly default settings are available to data subjects (privacy by default).[221]

Since these proposed reforms, which were intended to modernize the data protection statutes of EU Member States, including the DPA 1998, were first made public in January 2012,[222] the drafters of the 2013 bill should have given serious consideration to whether any of these reforms could have been incorporated into this bill.

E. The Personal Information and Data Protection Bill (Circa 2013)

There appears to be no formal record of the Personal Information and Data Protection Bill ("PIDP Bill")[223] in the list of proposed legislative measures emanating from the Nigerian National Assembly. Unlike the three bills considered above, the true provenance of the PIDP Bill is not entirely certain, although it appears from available media reports that it was drafted by a Committee on Personal Information and Data Protection Legislation, operating under the auspices of the National Identity Management Commission.[224] The Commission's main purpose is to carry out the enrollment

---

[217] *Id*. at arts. 33–34.

[218] EU GDPR, Regulation 2016/679 *supra*, note 1, at art. 35.

[219] *Id.* at art. 37.

[220] *Id.* at art. 25(1).

[221] *Id.* at art. 25(2).

[222] *See* Gerrit Hornung, *A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012*, 9(1) SCRIPTED 64, 64 (2012), https://script-ed.org/wp-content/uploads/2012/05/hornung.pdf.

[223] Personal Information and Data Protection Bill (2013) (Nigeria).

[224] *See* Onyebuchi Ezigbo, *Bill to Safeguard Personal Information Underway*, BIZCOMMUNITY (Feb. 25, 2013), http://www.bizcommunity.com/Article/410/15/89761.html*; see also Proposed Draft Bill on Personal Information and Data Protection (Excerpts from a keynote address by Mr. Mohammed Bello Adoke, SAN, CFR Hon. Attorney-General of Federation & Minister of Justice and Minister of Justice at the stakeholders workshop on the draft bill on personal information and data protection in Abuja),* para. 1, DIGITAL SENSE NEWS (Feb. 5, 2014),

of Nigerian citizens and legal residents, issue National Identity smart cards to enrollees, and create and manage a national identity database.[225] Section 31(2) of the National Identity Management Commission Act 2007 empowers the Commission to make regulations providing for the collection, collation, and processing of data and other relevant information.[226] It is presumably on the strength of this authority that it constituted the Committee to prepare the PIDP Bill.[227] It is not entirely clear when the bill was first drafted, but it came prominently into the public eye early in 2013 when the Commission convened a "Stakeholder's Conference" to deliberate on its provisions.[228]

The most intriguing feature of the PIDP Bill is that it has completely forsaken the model of the DPA 1998 and has instead been modeled very closely on Canada's PIPEDA.[229] The drafters of the PIDP Bill may have been attracted to the Canadian model because Canada has a federal system of government similar to Nigeria.[230] Canada's Bill has thus taken account of the constitutional allocation of legislative powers between Canada's Federal Parliament and its provincial Legislative Assemblies. Specifically, "PIPEDA was designed to work in tandem with provincial legislation" and "contemplates the harmonization of provincial and federal privacy protection."[231]

With this in mind, PIPEDA provides that where provincial legislation has been enacted with substantial similarity to PIPEDA, Canada's Governor-General may exempt organizations and activities that are subject to such provincial legislation from the operation of PIPEDA, with respect to the

---

http://digitalsenseafrica.blogspot.co.uk/2014/02/proposed-draft-bill-on-personal.html?m=0> [hereinafter *Proposed Draft Bill on Personal Information and Data Protection].*

[225] *See About Us,* NAT'L IDENTITY MANAGEMENT COMMISSION (2007), http://www.nimc.gov.ng/about-us/ (last visited Oct. 1, 2016).

[226] National Identity Management Commission Act, Chapter N154 Laws of the Federation of Nigeria 2010 (Nigeria), § 31(2).

[227] *See Proposed Draft Bill on Personal Information and Data Protection, supra* note 224 (highlighting the role of this committee in preparing the Personal Information and Data Protection Bill).

[228] *See* Ezigbo, *supra* note 224 (reporting on the Stakeholders Conference in which the bill was discussed).

[229] Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5 (Can.).

[230] *See* Constitution Act, 1867, 30 & 31 Vict. c 3 (U.K.), *reprinted in* R.S.C. 1985, app II, no 5, §§ 91 & 92 (Can.) ("Whereas the Provinces of Canada, Nova Scotia, and New Brunswick have expressed their Desire to be federally united into One Dominion…"); *cf.* CONSTITUTION OF NIGERIA (1999) § 2(2) ("Nigeria shall be a Federation consisting of States and a Federal Capital Territory").

[231] FRANCE HOULE & LORNE SOSSIN, OFFICE OF THE PRIVACY COMM'R OF CAN., POWERS AND FUNCTIONS OF THE OMBUDSMAN IN THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT: AN EFFECTIVENESS STUDY 114 (2010) (Houle and Sossin are two leading Canadian scholars who were commissioned by the Canadian Privacy Commissioner to evaluate whether the Ombudsman model provided by Personal Information and Electronic Documents Act was effective in regulating data privacy in Canada).

collection, use, and disclosure of personal information within that province.[232] Bastarache comments on the effect of this provision, stating, "PIPEDA contains federal-provincial cooperation mechanisms with regard to the protection of personal information. In essence, opting out of the application of PIPEDA for intra-provincial personal information practices is possible for provinces who have provincial legislation substantially similar to PIPEDA."[233] The drafters of the PIDP Bill inserted an almost identical provision, although in view of the fact that Nigeria—unlike Canada—is not a constitutional monarchy with a Governor-General, but a fully-fledged republic, the Nigerian President exercises the power of exemption instead.[234]

Another consideration which may have helped sway the drafters of the PIDP Bill towards the Canadian model was that the PIPEDA regime had been adjudged by the European Commission to confer an adequate level of protection on data processed in Canada.[235] This exempts Canada from the restrictions imposed by Article 25 of the EU DPD on the transfer of personal data from the EU to non-EU Member States. [236] It is conceivable that those responsible for the Nigerian Bill naively assumed that if the Nigerian Legislature re-enacted PIPEDA almost verbatim, the Commission would make a positive finding of adequacy in Nigeria's favor thereby facilitating the free flow of personal data from the EU to Nigeria with all its attendant commercial advantages.

Like PIPEDA, the PIDP Bill applies to organizations that collect, use, or disclose personal information in the course of their commercial activities.[237] It also applies in circumstances where organizations collect, use, or disclose personal information pertaining to their employees in connection with a federal work, undertaking, or business.[238] The PIDP Bill, however, exempts

---

[232] Personal Information Protection and Electronic Documents Act, 2000 S.C., c. 5, § 26(2) (b) (Can.).

[233] MICHEL BASTARACHE, THE CONSTITUTIONALITY OF PIPEDA: A RE-CONSIDERATION IN THE WAKE OF THE SUPREME COURT OF CANADA'S RE-REFERENCE SECURITIES ACT (2012), http://accessprivacy.s3.amazonawa.com/m-bastarache-june-2012-contitutionality-pipeda-paper-2.pdf (citing the Personal Information and Electronic Documents Act § 26(2) (Can.)); *see also* Jeremy Warner, *The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps,* 2 U. OTTAWA L. & TECH. J. 75, 93 (2005) (explaining that § 26(2) gives rise to a "relationship of mutual exclusivity" between the Personal Information and Electronic Documents Act at the federal level and substantially similar provincial laws).

[234] *See* Personal Information and Data Protection Bill (2013), § 28(2) (Nigeria).

[235] *See* 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, 2002 O.J. (L2) 13.

[236] *See* EU DPD, art. 25 (1) & 25(2).

[237] Personal Information and Data Protection Bill (2013), § 2(1) (Nigeria); Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, § 4(1) (Can.).

[238] Personal Information and Data Protection Bill (2013), § 2(1) (Nigeria).

government institutions, any information that an individual collects, uses, or discloses exclusively for personal or domestic purposes, and any organization with respect to personal information it uses exclusively for journalistic, artistic, or literary purposes.[239]

The PIDP Bill requires all non-exempt organizations to comply with obligations set out in Schedule 1, which contains a set of ten privacy principles that are virtually identical to the ten principles in Schedule 1 of PIPEDA.[240] These principles were originally part of the Privacy Framework set out in the Canadian Standards Association's 1996 Model Code for the Protection of Personal Information.[241] They require these organizations to seek the consent of individuals when collecting, using, or disclosing personal information pertaining to them.[242] In much the same way as PIPEDA does, the PIDP Bill identifies a wide range of situations in which personal information may be collected, used, and disclosed by such organizations without having to obtain consent.[243] The PIDP Bill also spells out in very similar terms to PIPEDA, the entitlement of individuals to request access to personal information relating to them, the corresponding obligation on the part of organizations to respond to such requests, and a range of circumstances in which access is prohibited or may be refused.[244]

The PIDP Bill provides precisely the same remedial framework as PIPEDA for individuals who allege that an organization has contravened a provision of the Bill or violated any of the principles in Schedule 1. The initial course of action open to them is to file a complaint with the Privacy Commissioner. The nature, scope, and limits of the investigatory, adjudicatory, and other powers exercisable by the Commissioner in response to such complaints are more or less identical in both cases.[245] The PIDP Bill also specifies exactly the same

---

[239] Personal Information and Data Protection Bill (2013), § 2(2) (Nigeria); Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, § 4(2) (Can.).

[240] Personal Information and Data Protection Bill (2013), § 3(1) (Nigeria) (mirroring Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, § 5(1) (Can.)).

[241] CAN. STANDARDS ASS'N, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION CAN/CSA-Q380-96 (1996), http://simson.net/ref/1996/CSA_Privacy_Standard_CSA-Q830-96.pdf.

[242] Personal Information and Data Protection Bill (2013), sched. 1, princ. 3 (Nigeria) (mirroring PIPEDA, *supra* note 8, at sched.1, princ. 3).

[243] Personal Information and Data Protection Bill (2013), § 5 (Nigeria); Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, § 7 (Can.).

[244] Personal Information and Data Protection Bill (2013), §§ 7–9 (Nigeria); Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, §§ 8–10 (Can.).

[245] Personal Information and Data Protection Bill (2013), §§ 10–14 (Nigeria); Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, §§ 11–13 (Can.). It is particularly noteworthy in this connection that both the Personal Information and Data Protection Bill § 12(2) and Personal Information Protection and Electronic Documents Act § 12(1) (2) explicitly empower the Commissioner to "attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation."

procedure for judicial recourse upon receipt of the Commissioner's report or upon notification that the commissioner discontinued the complaint. The remedies available to the court are also identical in both pieces of legislation.[246]

In embracing the Canadian model almost completely, the PIDP Bill's Nigerian proponents demonstrated no awareness of the groundswell of legitimate concerns and trenchant criticisms evoked by PIPEDA from its inception. In the first place, the drafters of the PIDP Bill chose to replicate *mutatis mutandis*, the formula in Article 26(2)(b) of PIPEDA, whereby PIPEDA could be excluded from applying to the processing of personal information within those Canadian provinces with substantially similar legislation.[247] In doing so, the Nigerian Legislature seems to have overlooked the fact that the constitutionality of PIPEDA has been disputed in various quarters on the ground that it breaches the scheme for the distribution of legislative powers established in the Canadian Constitution Act of 1867.[248] As Lawford points out, "PIPEDA took an interesting tack on the question of federal jurisdiction over privacy," and in doing so, it "seem[ed] to infringe significantly upon provincial constitutional competence."[249] The ensuing controversy has not yet been fully resolved by the Canadian judiciary, which should have given the drafters of the PIDP Bill pause when seeking to adopt the Canadian model.

Secondly, there is a fairly widespread perception that PIPEDA is more favorable to commercial organizations, whose collection, use, and disclosure of personal information PIPEDA seeks to regulate, rather than to the individuals whose personal information it ostensibly seeks to protect. Piper, for instance, refers to "the disproportionate and anti-democratic importance of business interests in the promulgation of the legislation."[250] She argues that the interests of the Canadian federal government were closely aligned with the self-interest of business groups, which led to legislation that protected the short-term needs of business stakeholders, rather than serving as an effective vehicle for establishing a long-term privacy framework that would promote the

---

[246] Personal Information and Data Protection Bill (2013), §§ 15–18 (Nigeria); Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, §§ 14–17 (Can.).

[247] *See* Personal Information and Data Protection Bill (2013), § 28(2) (Nigeria) ("The President may, by order, if satisfied that legislation of a State that is substantially similar to this Act applies to an organisation, a class of organisations, an activity or a class of activities, exempt the organisation, activity or class from the application of this Act in respect of the collection, use or disclosure of personal information that occurs within that State").

[248] Constitution Act, 1867, 30 & 31 Vict. c 3 (U.K.), *reprinted in* R.S.C. 1985, app II, no 5, §§ 91 & 92 (Can.).

[249] JOHN LAWFORD, PUBLIC INTEREST ADVOCACY CENTER, OTTAWA, CONSUMER PRIVACY UNDER PIPEDA: HOW ARE WE DOING? 7 (2004); *see also* Mahmud Jamal, *Is PIPEDA Constitutional?*, 43 CAN. BUS. L. J. 434, 438–39 (2006); BASTARACHE, *supra* note 233, 1–20.

[250] Tina Piper, *The Personal Information Protection and Electronic Documents Act: A Lost Opportunity to Democratize Canada's "Technological Society,"* 23 DALHOUSIE L.J. 253, 253 (2000).

public good.[251] Houle and Sossin reiterate this point and indicate that many felt the views of private business dominated the debates that preceded the enactment of PIPEDA and that the concerns of citizens were not well represented in those debates. They argue that this "is paradoxical given that the issue of those debates was the fundamental protection of personal information."[252] If the drafters of the PIDP Bill had been cognizant of such sentiments, they might have considered more carefully whether PIPEDA had struck the right balance between these competing imperatives before rushing to copy it so uncritically.

A further complexity arising from the PIPEDA regime relates to Schedule 1. MacDonnell describes the CSA Model Code,[253] as replicated in Schedule 1 of the Act, as an almost conversational document that introduces its ten principles and then elaborates on them.[254] According to McClennan and Schick PIPEDA has, as a result, been criticized for a lack of clarity since the intermittent use of "shall" and "should" in the model code has meant that some of its "ten commandments" are mandatory obligations and others mere recommendations.[255] This is not a particularly apt way of achieving the requisite degree of precision that should be the hallmark of sound legislation. Scassa points out that "Schedule 1 . . . consist[s] essentially of a reproduction *in toto* of the [CSA] *Model Code* . . . . [i]t is clear that a consensus-based voluntary code of this nature was never intended to provide the more strict normative guidance which one expects of legislation."[256] She further suggests that "[a]s a result of the way in which it has been drafted, with the adoption of the entire CSA Model Code as the normative heart of the legislation, PI[PE]DA is an unwieldy tool for the protection of personal information."[257] This difficulty was briefly alluded to in the context of the PIDP Bill by Banisar who asserts that it is a "primary concern . . . that the basic principles that govern the law have been subjected to a schedule in the back of the law rather than [appearing] in the main text."[258] The drafters of the PIDP Bill injudiciously fell

---

[251] *Id.* at 255.

[252] HOULE & SOSSIN, *supra* note 231, at 8.

[253] CAN. STANDARDS ASS'N, *supra* note 241.

[254] John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval*, 39 ALTA. L.R. 346, 373 (2001).

[255] Jennifer McClennan & Vadim Schick, *"O, Privacy" Canada's Importance in the Development of the International Data Privacy Regime*, 38 GEO. J. INT'L L. 669, 684 (2006–07).

[256] Teresa Scassa, *Text and Context: Making Sense of Canada's New Personal Information Protection Legislation*, 32 OTTAWA L.R. 1, 6 (2000–01).

[257] *Id.* at 33.

[258] David Banisar, *Nigeria: Personal Information and Data Protection Bill*, ARTICLE 19, 8 (Feb. 2013), https://www.article19.org/data/files/medialibrary/3683/Nigeria-Personal-Information-and-Data-Protection-Bill.pdf.

into this trap in spite of the concerns that have been voiced in Canada regarding the incorporation of the CSA scheme into Schedule 1.

Critics have also expressed considerable dissatisfaction regarding the perceived weakness of the enforcement mechanisms available under the PIPEDA regime. This has recently been acknowledged by the Canadian Privacy Commissioner who noted that "[t]he appropriateness of the current PIPEDA enforcement model has been the subject of debate prior to the law coming into force and in the ensuing years."[259] The problem emerged because PIPEDA opted for an Ombudsman model under which the Privacy Commissioner had very limited enforcement powers, which excluded order making powers and the ability to fine offenders.[260] Instead, the conciliatory role of the Commissioner encourages parties to solve their differences amicably.[261] Even though the Commissioner can suggest recommendations to the parties, he does not have the power to pronounce enforceable decisions. Therefore, respondents are not bound by the outcome.[262] Despite the concerns raised in Canada, the drafters of the PIDP Bill adopted precisely the same procedure. Banisar points out that while individuals are allowed to file complaints concerning violations of their rights, under the PIDP Bill "when it comes to enforcing these rights, the Commissioner's remedies seem to be limited to resolving complaints through dispute mechanisms such as mediation and conciliation."[263] Although an individual or the Commissioner may thereafter bring an enforcement action before the Canadian Federal Court and the Nigerian Federal High Court respectively,[264] Houle and Sossin highlight the costs generated by that procedure (over and above the costs of any initial complaint) and point out that "the two-step process is long and expensive [and] is liable to discourage complainants and reduce the number of cases which might be heard by the Federal Court."[265]

Another major structural criticism is that the PIDP Bill explicitly "does not apply to any government institution"[266] and has not been supplemented by any other legislation regulating the collection, use, and distribution of personal

---

[259] OFFICE OF THE PRIVACY COMM'R OF CAN., THE CASE FOR REFORMING THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT 5 (2013).

[260] *Id.* at 5–7.

[261] *See* Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5 §§ 12.1(1) & 12.1 (2) (Can.).

[262] THE CASE FOR REFORMING THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT, *supra* note 259, at 5. *See also*, LAWFORD, *supra* note 249, at 8.

[263] Banisar, *supra* note 258, at 11.

[264] *See* Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, §§ 14(1) & 15 (Can.); Personal Information and Data Protection Bill (2013), §§ 15(1) & 16 (Nigeria).

[265] HOULE & SOSSIN, *supra* note 231, at 10.

[266] *See* Personal Information and Data Protection Bill (2013), § 2(2)(a) (Nigeria).

information by government institutions. The corresponding section in PIPEDA stipulates that it "does not apply to any government institutions *to which the Privacy Act applies* [emphasis added]."[267] This provision is understandable in the Canadian statutory scheme since the Canadian Privacy Act of 1985 contains a parallel data privacy regime designed to "protect the privacy of individuals with respect to personal information about themselves held by a government institution and . . . . provide individuals with a right of access to that information."[268] However, there is currently no Nigerian statute corresponding to the Canadian Privacy Act. This means that enacting the Nigerian Bill in its current form would have the undesirable effect of placing public institutions above the law when it comes to data protection. Commenting on this state of affairs, Banisar asserts that:

> [t]he most significant flaw in the law is its apparent application only to the private sector . . . . This is a serious problem given the lack of a detailed law on the collection, use and disclosure of personal information law in Nigeria. It leaves mostly unprotected from abuse the records of millions of citizens including the medical records, identity information and anything else held by public bodies.[269]

The mechanical manner in which PIPEDA has been copied by the PIDP Bill has also given rise to one or two relatively minor, but nonetheless irritating, drafting anomalies. The first concerns the definition of "personal health information" in PIPEDA[270] that is repeated verbatim in the definition section of the PIDP Bill.[271] The reason why it was necessary for this definition to appear in PIPEDA was because it contained transitional provisions providing for its operation to be phased into the health sector. Therefore, PIPEDA stipulated that it would only affect personal health information collected, used, or disclosed by an organization one year after the day on which PIPEDA was enacted.[272] By contrast, the PIDP Bill does not include any corresponding transitional provisions, and since there is no reference to personal health information anywhere else within the bill, its inclusion in the definition section is entirely superfluous and constitutes a rather careless oversight.

---

[267] Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, § 4(2)(a) (Can.).

[268] Privacy Act, R.S.C., 1985, c P-21, § 2 (Can.).

[269] Banisar, *supra* note 258, at 8.

[270] Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, § 2 (Can.).

[271] Personal Information and Data Protection Bill (2013), § 33 (Nigeria).

[272] Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, §§ 30(1.1) & 30(2.1) (Can.). PIPEDA came into force in January 2001, meaning that its application to the health sector was delayed until January 2002. *See* David T.S. Fraser, *The Application of PIPEDA to Personal Health Information*, CAN. PRIVACY L.R. n. 2 (2004), http://www.privacylawyer.ca/privacy/pipeda_and_personal_health_information.pdf.

The second drafting anomaly that is evident in the PIDP Bill arises from the fact that the privacy principles set out in Schedule 1 of PIPEDA are serially enumerated from 4.1 to 4.10. This particular form of enumeration is attributable to the fact that the principles originate from Part 4 of the CSA Model Code that was incorporated *verbatim* into this Schedule.[273] Indeed, this is explicitly acknowledged in PIPEDA Schedule 1, which is entitled "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96."[274] The drafters of the PIDP Bill adopted the same form of enumeration in PIPEDA's Schedule 1, and the seemingly random reference to Principles 4.1 to 4.10 in the Nigerian version will likely be a source of confusion as the connection to the CSA Model code is not made clear in the Schedule. Therefore, Banisar is justified in asserting "[o]verall, the bill is poorly drafted and includes many inconsistent and conflicting provisions as well as a general difficulty in understanding which will seriously undermines its effectiveness."[275]

Furthermore, after the PIDP Bill was initially introduced, the Canadian Parliament enacted the Digital Privacy Act.[276] This Act amended the version of PIPEDA that formed the basis of the Nigerian version in several significant respects. For example, the Act strengthened the consent requirement in PIPEDA by specifying that such consent will now be valid, only if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purposes, and consequences of the collection, use, or disclosure of the personal information to which they are consenting.[277] Another key provision of the new Act makes it incumbent on organizations to report to the Privacy Commissioner any breach of security safeguards involving personal data under their control, if there is reason to believe that the breach creates a significant risk of harm to an individual.[278] Moreover, the 2015 Act fortifies the relatively weak enforcement procedures in PIPEDA, by equipping the Privacy Commissioner with an additional means of prevailing on organizations engaged in the processing of personal information to adhere to their PIPEDA obligations.[279] More specifically, it empowers the Commissioner to enter into compliance agreements with organizations that he or she has reason to believe have committed, or are likely to commit, breaches

---

[273] CAN. STANDARDS ASS'N, *supra* note 241.

[274] *See* Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, sched. 1, § 2 (Can.).

[275] Banisar, *supra* note 258, at 8.

[276] Digital Privacy Act, S.C 2015, c 32 (Can.).

[277] *Id.* § 5.

[278] *Id.* § 10.

[279] *Id.* § 15.

of PIPEDA.[280] Such agreements may contain any terms the Commissioner deems necessary and the Commissioner may, if the need arises, go to court to ensure compliance with the agreement.[281] Even though many of the amendments in the Digital Privacy Act were available to the public and were being discussed in Canadian legal reform circles at the time the Nigerian draft was produced, the discussion did not come to the attention of the drafters of the PIDP. It follows that if the PIDP is enacted in its current form, it will not benefit from any of the recent modifications to PIPEDA.

The inadequacy of the PIDP Bill becomes even more obvious when it is contrasted with Singapore's Personal Data Protection Act 2012 ("the Singaporean Act"), which also bears some of the hallmarks of the Canadian PIPEDA model.[282] For example, the declared purpose of the Singaporean Act is virtually the same as that set out in PIPEDA.[283] Again, it is noticeable that the objective standard of "what a reasonable person would consider appropriate in the circumstances" against which PIPEDA evaluates the collection, use, and disposal of personal information has also found its way into the Singaporean Act.[284]

Despite such similarities, the Singaporean Act has sought to mitigate some of the more unsalutary features of PIPEDA. First, instead of merely incorporating the vague, nebulous mish-mash of obligatory principles and mere recommendations that make up the CSA Model Code, the Singaporean approach has been to distill them into a precisely drafted set of general rules that are contained in Parts III–VI.[285] Second, under the Singaporean Act, the Personal Data Protection Commission possesses much greater powers of enforcement against errant organizations than the Office of the Privacy Commissioner does under PIPEDA.[286] There is some scope for mediation built into the enforcement provisions of the Singaporean Act,[287] but the Commission is also given the power to review, countermand, or disallow decisions

---

[280] *Id.* § 15(1).

[281] Digital Privacy Act, S.C 2015, c 32, § 15(2) (Can.).

[282] Personal Data Protection Act 2012 (2012 S.S. 26) (Sing.) http://statutes.agc.gov.sg/aol/download/0/0/pdf/binaryFile/pdfFile.pdf?CompId:ad8fc392-68d2-4eab-a419-9f34f876b505. For a more in-depth analysis of the Singaporean Act, *see* GREENLEAF, *supra* note 10, at 289–315; Simon Chesterman, *From Privacy to Data Protection, in* DATA PROTECTION LAW IN SINGAPORE: PRIVACY AND SOVEREIGNTY IN AN INTERCONNECTED WORLD 1, 22–41 (Simon Chesterman ed., 2014).

[283] *See* Personal Data Protection Act 2012 (2012 S.S. 26) § 3 (Sing.); Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, § 3 (Can.).

[284] *See* Personal Data Protection Act 2012 (2012 S.S. 26), § 13 (Sing.); Personal Information Protection and Electronic Documents Act, 2000 S.C., c 5, § 5(3) (Can.).

[285] Personal Data Protection Act 2012 (2012 S.S. 26), §§ 11–26 (Sing.).

[286] *Id.* §§ 28 & 29 (power to review complaints).

[287] *Id.* § 27 (alternative dispute resolution).

concerning refusals to provide access to personal data, to charge fees for such access, or to correct erroneous personal data.[288] The Commission is also vested with the power to stop errant organizations from "collecting, using or disclosing personal data . . . ." and may also require organizations "to destroy personal data collected . . ." by them, and to pay financial penalties of up to $1 million.[289]

The authors of the Singaporean Act have also ventured beyond the legislative terrain staked out by PIPEDA in various other significant respects. For instance, unlike PIPEDA, which does not contain any specific adequacy provisions relating to data exports, the Singaporean Act explicitly curtails the transfer of personal data to other countries that do not provide sufficient protections for personal data so transferred. This provision is similar to the adequacy requirements specified by the United Kingdom's eighth data protection principle and Article 25(1) of the EU DPD.[290] Again, unlike PIPEDA, the Singaporean Act creates an elaborate appellate structure to deal with data protection disputes. Organizations or individuals that are aggrieved by the Commission's decisions and directions may bring their case to a special Data Protection Appeal Panel established under the Singaporean Act.[291] Further, a channel is provided for additional appeals to the High Court and beyond.[292] A comparison of the Singaporean Act and the PIDP Bill suggests that Singapore's legislators are more highly sophisticated and much more adept at negotiating the niceties and complexities of legal transplantation than their Nigerian counterparts.

F. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes Act 2015 is concerned with the prohibition, prevention, detection, prosecution, and punishment of cybercrimes.[293] In addition, however, the Act specifies that one of its objectives is "*[t]he protection of* . . .

---

[288] *Id.* § 28 (power to review).

[289] *Id.* § 29 (power to give directions).

[290] Personal Data Protection Act 2012 (2012 S.S. 26), § 26 (Sing.) (transfers of personal data outside Singapore).

[291] *Id.* §§ 33–34.

[292] *Id.* § 35.

[293] The Cybercrimes Act 2015 (2015) (Nigeria), https://cert.gov.ng/images/uploads/CyberCrime_%28Prohibition%2CPrevention%2Cetc%29_Act%2C_2015.pdf. After sluggish progress over the years, this Bill is reported to have been hurried through the Nigerian National Assembly in a whirlwind of legislative activity that marked the last day in office of Nigeria's immediate past President, Goodluck Jonathan, along with forty-five other Bills. *See* Femi Daniel, *Nigeria*: *Cybercrimes Act 2015 - Legal Risk Exposures of Information Technology Companies,* THE GUARDIAN (Feb. 9, 2016), http://allafrica.com/stories/201602090041.html ("the Nigerian 7th National Assembly would go down as one of the most sensational gathering[s] of eminent Nigerians ever. One of its feats was the world-record breaking feat of passing 46 Bills within 10 minutes on its last legislative day" including the Cybercrime Act 2015).

data and computer programs, intellectual property and *privacy rights*," thereby conveying the impression that regulation of data privacy is one of its chief concerns.[294] This impression is reinforced by a subsequent section of the Cybercrimes Act ostensibly concerned with "[r]ecords retention and protection of data."[295] A closer look at this section, however, reveals that this reference to "protection of data" is somewhat misleading since the main thrust of the section is not to safeguard the interests of data subjects. Rather, the focus of this section of the Cybercrimes Act is to assist the nation's law enforcement agencies in tackling cybercrimes by ensuring that providers of digital services (1) retain and preserve any traffic data, subscriber information, and content data pertaining to their users for at least two years and (2) make such information available at the request of these agencies.[296]

Although the Cybercrimes Act focuses on tackling cybercrime, the Act also ostensibly provides basic protections for individual data subjects. Specifically, the Act insists that personal information "shall not be utilized except for legitimate purposes,"[297] and that data users must respect individual privacy rights as established in the Nigerian Constitution. Further, the Act requires that data processors take appropriate steps to maintain the confidentiality of data retained, processed, or retrieved for law enforcement purposes.[298] However, these protective provisions are severely curtailed because the Act goes on to stipulate that every provider of digital services must disclose any information requested by any law enforcement agency, without introducing any accompanying safeguards like judicial or administrative oversight.[299] Thus, it seems, contrary to the perceived objective of protecting privacy rights, the Cybercrimes Act is not designed to enhance the data privacy rights of individuals in any meaningful way.

V. CONCLUSION

Although the age of global conquest and colonization has now receded into history, in the case of Nigeria, the laws transplanted during the colonial period have exhibited a remarkable degree of longevity. In particular, the ongoing quest for a suitable data protection regime reveals that the present-day Nigerian legal system remains deeply tied to its colonial heritage. Further, Nigeria's regulatory authorities are still instinctively primed to seek legislative solutions from the "motherland" when confronted with complex new challenges arising from modern technology. The approach adopted by the Nigerian National Assembly when it has relied on English law has been disappointing.

---

[294] Cybercrimes Act 2015 (2015) (Nigeria), § 1(c) (Sing.) (emphasis added).

[295] *Id.* § 38.

[296] *Id.* §§ 38(1)–(3).

[297] *Id.* § 38(4).

[298] *Id.* § 38(5).

[299] Personal Data Protection Act 2012 (2012 S.S. 26) § 40(1) (Sing.).

Simply churning out bills like the Data Protection Bill 2011 and the Electronic Transactions Bill 2013 that merely replicate key aspects of the U.K. DPA 1998 reflect poorly on the creativity and perspicacity of Nigeria's legislators. It is also unfortunate that the Nigerian drafters of the 2013 Bill overlooked the fact that the EU DPD, which the DPA 1998 sought to implement, is currently in the throes of major reform and failed to address such changes in drafting their own bill.

The results have been just as disappointing for the three legislative measures not derived from the DPA 1998, namely the Cyber Security and Data Protection Agency Bill 2008, the Cybercrimes Act 2015, and the PIDP Bill. The Cyber Security and Data Protection Agency Bill 2008 and the Cybercrime Bill 2015 contain misleading buzzwords like "data protection" and "privacy," when they have done nothing to advance the cause of data privacy in Nigeria.

The PIDP Bill represents a marked departure from the norm on the Nigerian legislative front. Although Nigeria and Canada share the same common law heritage, there are no previous examples of the former having derived any substantial legislative guidance from the latter. The Nigerian legislature's decision to mimic the Canadian PIPEDA instead of the U.K. DPA is valid only so long as all other legislative options have been carefully considered. It is "fortunate that laws are not protected by copyrights, so that jurisdictions are free to pick and choose as they wish from the plethora of legal solutions already applied in other places."[300] Regrettably however, the drafters of the PIDP Bill construed this liberty as license to plagiarize the Canadian statute on a grand scale and pass it off as the product of their own earnest endeavors.[301] This matter is made worse because the PIDP Bill does not take into account recent Canadian reforms and is therefore nothing more than an outdated version of Canadian legislation.

Nigeria's regulatory elites have floundered in their attempts to devise a workable data protection regime for the nation. It is thus scarcely surprising that apart from the Cybercrimes Act 2015, none of their legislative proposals have so far made it to the statute book. This is particularly perplexing since other African countries such as Ghana and South Africa—which are at a similar stage in their legal development—have recently achieved a more satisfactory legislative outcome by adopting a more measured and meticulous approach to the task at hand.[302] An examination of the data protection statutes enacted by these two nations reveals they are more coherent, better structured,

---

[300] Michal S. Gal, *The Cut and Paste of Article 82 of the EC Treaty in Israel: Conditions for a Successful Transplant*, 9 EUR. J. L. REFORM 467, 484 (2007).

[301] It is however noteworthy that this is by no means an uncommon practice, a point emphasized by Fedtke, *supra* note 15, at 52 ("There is, of course, no obligation for legislators or judges who use foreign law to disclose the intellectual ownership of a legal idea and the origin of a rule (or indeed the fact that it was borrowed at all) will usually remain more or less obscure.").

[302] *See* Protection of Personal Information Act (Act No. 4/2013) (S.Afr.); Data Protection Act (Act No. 843/2012) (Ghana).

and far more comprehensive than any of the Nigerian bills because they do not simply replicate the contents of statutes in force in other jurisdictions. Unpalatable as this might be, it now seems incumbent on Nigeria's legislators to go back to the drawing board, and devote more time, energy, and intellectual effort to devising a data protection scheme that is worthy of its name.

This is not to suggest that Nigerian legislators ought to "reinvent the wheel," as this would consume an inordinate amount of the nation's limited legislative resources. Rather, there are several more feasible courses of action. First, they may wish to direct their legislative borrowing towards either Ghana or South Africa, since these are two nations which are within the same geographic region as Nigeria and whose current social, political, and economic circumstances are broadly similar. The main stumbling block here is that the Nigerian National Assembly might consider it *infra dignitatem* to yield in this or any other matter to the superior legislative wisdom of the Ghanaian or South African parliament. Secondly, given that Nigeria is a leading member of both ECOWAS and the AU, it would be perfectly legitimate for its legislators to seek to promote sub-regional or regional legal harmonization by devising a statutory data protection framework that is closely modeled on the ECOWAS Supplementary Act or the AU Convention. A third possibility might be for Nigeria to venture further afield and take a leaf out of the statute book of a country such as Singapore whose data protection legislation is infused with elements of the Canadian PIPEDA regime, while at the same time retaining a distinctly Singaporean flavor.

Whichever foreign model they eventually decide to embrace, the Nigerian authorities would do well to pay heed to three eminently sensible recommendations put forward by Makulilo.[303] The first is that the adoption of a data protection law in Africa should not be treated as a mere exercise in "cut and paste" of EU law or that of its member states (or indeed any other foreign legislation). The second is that the drafting of data protection legislation should not be left entirely to government or parliamentary drafting departments, but should also involve substantial input from leading experts in data protection law. The third is that in enacting data protection legislation, African governments must bear in mind that it is not solely a device for attracting foreign investment, but also an instrument for safeguarding their citizens against the infringement of their privacy rights.

---

[303] Makulilo, *supra* note 3, at 50.