‘Adequate protection’: An analysis of Nigeria’s data protection laws within an emerging global data protection framework

by

Adekunle Adewumi

LL.B, Afe Babalola University, 2016

**A Thesis Submitted in Partial Fulfillment
of the Requirements for the Degree of**

MASTER OF LAW

in the Faculty of Law

We acknowledge and respect the lək̓ʷəŋən peoples on whose traditional territory the university stands and the Songhees, Esquimalt and W̱SÁNEĆ peoples whose historical relationships with the land continue to this day.

‘Adequate protection’: An analysis of Nigeria’s data protection laws within an emerging global data protection framework

by

Adekunle Adewumi

LL.B, Afe Babalola University, 2016

Supervisory Committee

Dr. Patricia Cochran, Supervisor
Department of Law

Dr. Michelle Bonner, Co-supervisor
Department of Political Science

Abstract

The implementation of the European Union's General Data Protection Regulation in 2018 appeared to be the catalyst for several countries to take data protection seriously, owing to concerns about transborder data flow restrictions, and has resulted in the global expansion of data protection laws. One of such countries is Nigeria, whose National Information Technology Development Agency (NITDA) introduced the Nigerian Data Protection Regulation (NDPR) in 2019. Nigerians are becoming more aware of the need to protect their personal data, and while the NDPR fulfils the need for a data protection law, it does not automatically mean that personal data of data subjects is adequately protected within Nigeria. Due to the lack of internationally binding data protection agreements, determining what constitutes an "adequate" data protection framework is challenging. The GDPR currently maintains the highest data protection standard and provides an assessment criterion in Article 45(2) for determining whether countries outside the EU have adequate data protection frameworks.

In this regard, I assess how "adequate" Nigeria's data protection framework is in terms of the GDPR assessment criteria in Article 45(2). The Nigerian case is then compared to the Canadian data protection framework, which has received an adequacy decision from the EU. Based on this comparison, I make recommendations that, if implemented, will lay the groundwork for a data protection regime that meets the needs of Nigerian data subjects.

Table of Contents

Acknowledgements

I am eternally grateful to my supervisory committee, Professors. Patricia Cochran and Michelle Bonner, whose support and guidance was critical in assisting me to improve my research and writing skills and actively worked with me to achieve my aim of completing this dissertation within the timeframe agreed upon. I appreciate that my supervisory committee was always available to support me, even on short notice, and that they provided detailed feedback that helped me improve this dissertation.

I am grateful for the assistance I received from the University of Victoria Faculty of Law. I am especially grateful to Professor Rebecca Johnson, my LL.M seminar course instructor, for her very insightful classes, and I also thank Dr. Sara Ramshaw for her comments on a draft chapter of this dissertation, which helped guide my research. A significant portion of my time at UVIC was spent taking seminars in the Political Science faculty, and this experience was critical to the interdisciplinary nature of this research. I am grateful to have had the opportunity to take classes and learn from Professor Colin Bennett, whose invaluable experience provided deeper insight and motivated me to pursue this research further. I am also grateful to Tiffany Gordon, who was always available to answer my many questions, and to the other staff and faculty members of the UVIC Faculty of Law who supported me in various ways and helped to make my LL.M programme memorable.

While my dissertation promotes autonomy, I am fully aware that I am a product of a close-knit community that has supported me and without whom I would not be here. Thanks to my parents, Mr. and Mrs. Adewumi, whose love, prayers, and feedback kept me going. I want to thank my uncle Mr. Abiodun Agbele and brother Dele Adongbede who helped make this process more comfortable, I appreciate all your love and care. Thanks to Alejandra Brown, for her understanding and support when it was needed. Thank you to my friends Raphael Esu, Emmanuel Okpo-Ene, for being amazing and for your support throughout this program. I also want to appreciate Oreoluwa Ibrahim, who has been a fantastic partner on this journey.

Finally, I want to express my gratitude to God, through whose strength I have been able to do all things.

Dedication

Dedicated to the netizens who are committed to securing Nigeria's future.

CHAPTER 1: INTRODUCTION- 'ADEQUATE PROTECTION': AN ANALYSIS OF NIGERIA'S DATA PROTECTION LAWS WITHIN AN EMERGING GLOBAL DATA PROTECTION FRAMEWORK

1.0 Research Overview

The transborder flow of personal data has evolved into a key aspect of global trade and the lifeblood of a globalized economy.[1] This underpins the functions of governments, firms, and individuals who utilize it to execute a variety of tasks ranging from algorithms used by technology companies that power personal recommendation systems to the identity management and immigration control programs of various countries. Rapid technological evolution indicates that digital trade and transborder data flows will continue to grow, with data being optimized to create value.[2] The increased value placed on personal data has raised concerns about how informational privacy rights can be adequately protected while also considering the commercial, legal, and political issues associated with its use. Privacy concerns have also increased the number of countries that have enacted regulations that make data transfer more expensive and laborious, and in certain cases unlawful.[3]

The evolving regulatory framework has seen diverse data protection mechanisms adopted across various jurisdictions. This has created a complex and inconsistent regulatory landscape further exacerbated by the lack of internationally recognized standards.[4] However, there have been attempts made to fill the regulatory gaps by guidelines developed by intergovernmental organizations as well as legislation in countries that have prioritized data protection.[5] In this regard,

---

[1] Christopher Kuner, *Transborder data flows and data privacy law* (Oxford, United Kingdom: Oxford University Press, 2013) at 2.

[2] *Ibid* at 2.

[3] Richard Taylor, "Data Localization: The Internet in the Balance" (2020) 44:8 Telecommunications policy 1-15 at 9.

[4] Kuner, *supra* note 1 at 6.

[5] Peter Blume, "Transborder Data Flow: Is there a Solution in Sight?" (2000) 8:1 International Journal of Law and Information Technology 65–86 at. 84.

the European Union's (EU) General Data Protection Regulation (GDPR), clearly establishes the highest standards for all data protection laws.[6] These standards have theoretically given individuals more control over their personal information, increased penalties for companies that fail to provide adequate privacy protection policies, and provided mechanisms for redress where privacy rights have been violated.[7]

Article 45 of the GDPR, restricts the transfer of personal data outside the EU based on a decision as to whether such data is adequately protected [8] This section incorporates a number of requirements for evaluating the level of data protection provided by a third-country, territory or international organization.[9] This evaluation by the European Commission results in an "adequacy decision" that allows data export from the EU, and such export does not require any further specific authorization for transfers.[10] The commercial necessity for the transborder data flows to the EU has seen the GDPR have an "extraterritorial" effect on the reform of privacy protection laws beyond Europe and has influenced the development of an international data protection framework.[11]

Despite years of development in international data protection frameworks, African countries have been slow to adopt informational privacy laws and data rights protection mechanisms.[12] However, considering the effect of the GDPR and the economic expediency of implementing legislation, there has been a significant increase in the development of data

---

6 Aysem Vanberg, "Informational privacy post GDPR – end of the road or the start of a long journey?" (2021) 25:1 The International Journal of Human Rights 52-78 at 59.

7 Ibid at 61.

8 .EC, Regulation (EU) 2016/679 of the European Parliament and of the Council 2016/679 of 27 April 2016 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) [2016] OJ, L 119/1 p. 1-88.

9 *Ibid* at Art 45(2).

10 European Commission, Adequacy decisions (10 April 2021), online: European Commission https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/M2SQ-FYYY].

11 Benjamin Greze, "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives" (2019) 9:2 International Data Privacy Law 109-128 at 109.

12 Alex Makulilo, *The Future of Data Protection in Africa, in African data Privacy laws* (Cham, Springer International Publishing, 2016) at 378.

protection regulations across Africa. Keeping in tandem with this trend, The Nigerian Data Protection Regulation (NDPR) was an immediate response by Nigerian regulators to the effects of the GDPR.[13] The regulation provides an updated data protection mechanism that complements existing laws related to informational privacy and data rights in Nigeria.[14] It also aims to ensure businesses registered within its jurisdiction remain competitive in international trade.[15]

In most cases, enacting data protection legislation is considered a primary indicator of a jurisdiction's commitment to data protection, however, this alone is insufficient to determine whether a third country's data protection regime is adequate. The GDPR's Article 45(2) adequacy criteria provide a broader framework for carrying out such an assessment in this context. This dissertation, therefore, asks if Nigeria's legal and regulatory framework is "adequate" in light of increasing international data protection standards. While Nigeria has not sought an adequacy decision from the EU, it has recently made efforts to develop data protection standards in conformity with the GDPR and be compliant with European standards. In this regard, the requirements for obtaining an adequacy decision present an assessment criterion to determine whether current efforts are adequate.

In determining how adequate Nigeria's data protection framework is, I limit the definition of adequacy to what is established under Article 45(2) which provides that:

> When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security,

[13] Nigerian Data Protection Regulation, 25th January 2019 at Preamble.
[14] *Ibid*.
[15] *Ibid* at Art.1.1 (d).

> defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.[16]

I further identify comparable data protection standards in Canada, a jurisdiction with a similar legal system that has received a positive adequacy decision.[17] This comparison seeks to identify existing data protection practices deemed adequate by the European Commission (EC), as well as to provide insight into the gaps in Nigeria's data protection framework. Based on an

[16] GDPR, *supra* note 8 at Art.45(2).

[17] Commission Decision (EC) 2002/2 of 20 December 2001 pursuant to Directive (EC) 95/46 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] OJ L2/13.

assessment using the Article 45(2) GDPR criteria, a key finding in this dissertation is that, while Nigeria is at the foundational stage of developing a data protection framework, its current framework cannot be considered "adequate" because of significant gaps, such as disregard for the rule of law, limitations of the NDPR, a lack of an established redress mechanism for data subjects, and failure to respect international commitments. However, in comparison to the Canadian Data Protection Framework, I find that, while there is an existing need for reforms, there are important lessons that, if adopted by Nigerian regulators, may increase their chances of receiving an adequacy decision. This dissertation concludes by proposing practical solutions for Nigeria to improve its chances of developing a data protection framework that is considered "adequate".

1.1 Problem Context

Technological advancement and the proliferation of the internet has contributed to the rise of interconnectivity and integration of social, economic, and political systems worldwide. This has facilitated a surge in the nature and scope of data transfers which includes transborder data flows that have become a commercial necessity and vital for international trade. While the global digital economy is projected to account for 25% of global GDP by 2030, exceeding general economic growth, developing countries like Nigeria currently lag because they only account for a small share of this rise.[18] Nigeria's failure to invest strategically in the foundational elements of its digital economy through the establishment of a resilient and operational regulatory framework that facilitates a conducive business climate is one of the main reasons for this setback.[19]

An operational framework that has aided the growth of the digital economy is the evolution of data protection mechanisms and informational privacy laws at national and transnational levels,

[18] Musa Shuaib, "The Changing Pattern of International Trade: Import Substitution Policy and Digital Economy in Nigeria. A Review" (2020) 6:4 International Journal of Economics and Business Management 13-25 at 19.
[19] *Ibid* at 19.

which govern the transfer of personal data outside of the country where it was collected and processed.[20] Where distinct data protection laws and processes exist across jurisdictions, the fluidity and ubiquity of transborder data flows pose difficulties in deciding which legal regime to comply with. This is complicated further by the lack of a comprehensive international framework for data protection, as there are no binding data protection commitments or treaties that provide guidelines on the regulation of transborder data flows globally, in contrast to framework conventions established by the United Nations on other specific subject matters.[21]

The void created by the lack of an international framework influenced the development of other mechanisms, led by the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[22] which developed privacy standards that were later reflected in specific legislation such as the Data Protection Directive of the European Union (DPD).[23] The E.U Directive recognized the challenges posed by transborder data flows and imposed limitations on the transfer of personal data to third countries that did not provide an adequate level of protection.[24] It had the goal of harmonizing data processing rules across member states by ensuring that data processors did not bypass higher European standards through the export of personal data to countries with weaker levels of data protection. The prominence of the EU as a trade bloc created the necessity for countries to obtain adequacy decisions to facilitate the smooth flow of personal data, which encouraged other countries to implement data protection legislation comparable to those in the EU.

---

[20] Kuner, *supra* note 1 at 3.

[21] *Ibid* at 160.

[22] OECD, Council of the OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980). This spurred the creation of other privacy principles such as the Model Code for the Protection of Personal Information by the Canadian Standards Association (CAN/CSA-Q830-96; published March 1996; reaffirmed 2001).

[23] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to processing of personal data and on the free movement of such data, 24 October 1995, OJ L 281/31.

[24] *Ibid*, at Art.25(1).

Going beyond the notion of adequacy which was established in 1995, the GDPR has replaced the directive, significantly standardizing the provisions that governed transborder data flows and giving European standards an even greater international significance.[25] Article 45(1) of the GDPR defines the regulation's default principle for the export of personal data, specifying that any data export to a country outside the EU is only allowed if the European Commission has provided a decision considering the recipient's country's data protection framework as adequate or in the absence of this, where additional safeguards exist. Article 45(2) of the GDPR, provides for specific requirements which the European Commission (EC) must take into account before reaching an adequacy decision.

The flow of information and data between countries is crucial for economic sustainability and vitality. As a result, data export legislations recognise territorial borders, but it also puts transborder data flows in jeopardy. Various countries have implemented data protection laws that are comparable to the GDPR; nonetheless, the existence of regulations alone is insufficient in determining whether these countries' data protection standards are "adequate".[26] It is also important to note that the requirements for obtaining adequacy decisions are based on relatively high standards as just 12 countries have received positive adequacy decisions since European data protection regulations were introduced in 1995. Despite attempts made by a limited number of African countries to obtain an adequacy decision, there has not been any positive adequacy finding on the continent, and it is expected that fewer countries are likely to meet the criteria under the GDPR.[27]

---

[25] Michelle Goddard, "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact" (2017) 59:6 International Journal of Market Research 703-705 at 704.

[26] Julian Wagner, "The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?" (2018) 8 International Data Privacy Law 318-337 at 321.

[27] Alex Makulilo, "The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius" (2020) 25:1 International Journal of Human Rights 117-146 at 125.

Nigeria's drive to position itself as a player in the global digital economy, as previously said, necessitates a commitment to providing an enabling environment for industry to thrive. One of these measures is to ensure that it complies with international data privacy standards by enacting its laws. Prior to the NDPR, most laws that covered data protection in Nigeria were sectoral.[28] The NDPR which was introduced by the National Information Technology Development Agency (NITDA) in 2019 by virtue of its statutory mandate under the NITDA Act of 2007:

> to develop regulations for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labor and other fields, where the use of electronic communication may improve the exchange of data and information.

Since the introduction of the NDPR, the implementation and enforcement of data protection regulations has been difficult and fraught with ambiguity; thus, NITDA took the initiative in July 2019 by releasing the Nigeria Data Protection Regulation 2019: Implementation Framework (the Draft Framework) to assist organizations in complying with the NDPR.[29]

Makulilo notes that, despite advances in regulatory standards, there is still a long way to go in developing strong and resilient data protection frameworks in Africa.[30] This is also true in Nigeria, where Salami identifies that attempts are currently underway to develop a more comprehensive data protection legislation.[31] However, Nigeria is still beset by inadequate data

---

[28] Emmanuel Salami, "Nigerian Data Protection Law: The Effectiveness of the Nigerian Data Protection Bill as a Tool for Fostering Data Protection Compliance in Nigeria" (2019) 43:9 Datenschutz und Datensicherheit 575-582 at 576.

[29] National Information Technology Development Agency Act, LFN 2007, c.28. The National Information Technology Development Agency was established with the mission of developing a framework for planning, research, development, standardization, application, coordination, monitoring, evaluation, and regulation of information technology practices, activities, and systems in Nigeria, among other things. The agency retains supervisory jurisdiction for data protection in Nigeria due to the lack of an independent data protection body.

[30] Alex Makulilo, *supra* note 12 at 378.

[31] Salami, *supra* note 28 at 576.

protection enforcement, the limited role of the judiciary in developing privacy jurisprudence, illegal data practices, including the processing of personal data without a legal basis, illicit data sales, commoditization of data subjects and their data, and unregulated data retention and transfer.[32] Developing legislation is clearly the easy part of protecting personal data within a jurisdiction, and this dissertation evaluates the adequacy of Nigeria's data protection system in the context of the GDPR's evaluation standards in Article 45(2).

1.2 Literature Review

Data protection is an evolving subset of the privacy discourse that has grown in importance as technology innovation and cross-border trade have progressed. This has sparked an increase in interest and research into the impact of cross-border data flows on personal data protection on a global scale. However, Makulilo emphasizes that the subject of data protection on the African continent is relatively new, stating that data privacy regulations are not indigenous to African countries and are primarily imported from western countries.[33] He further argues that the need for African countries to secure better opportunities for offshoring business from Europe is a major reason why African countries have adopted or intend to adopt comprehensive data protection laws.[34] Specifically referencing Nigeria, Babalola notes that data protection has a checkered history, with numerous failed attempts to develop a comprehensive data protection law, a lack of political will, and also an ineffective system for seeking judicial redress.[35]

Internationally, the data protection literature falls into various categories, with much interest in its concept as a human right and its relationship with the right to privacy. While there are significant overlaps in the scope of both rights, Kokott & Sobotta point out that there is a

[32] *Ibid* at 575.
[33] Alex Makulilo, *supra* note 12 at 20.
[34] *Ibid.*
[35] Olumide Babalola, "Nigeria's data protection legal and institutional model: an overview" (2021) 0:0 International Data Privacy Law 1-9 at 2.

tendency to treat the right to data protection as an expression of the right to privacy. However, the distinction between the two rights in the EU Charter of Fundamental Rights (ECHR) is not purely symbolic, as there are major areas where their personal and substantive scope diverge.[36] Early research by privacy scholars focused primarily on the right to privacy, with data protection being subsumed within the discourse. However, the impact of the GDPR on international data transfer has significantly influenced more scholarly research in the economic and political effects of data protection regulations.

Mannion asserts that with the GDPR the EU took a firm "take it or leave it" approach, requiring countries that want access to European markets to pass domestic laws that comply with the GDPR's expansive data obligations or risk losing access.[37] While establishing compliance may be easier for developed countries, Curtiss contends that developing countries are more likely to lack technological sophistication, national privacy regimes, or effective judicial systems, and these flaws pose significant threats to the security of personal information in the data-sharing chain.[38] Makulilo also notes that the standards for assessing third countries may be flawed because, in practice, they have taken into account extraneous considerations not contemplated by European regulations, such as broad political negotiations that precede any adequacy assessment.[39]

Assessing the extraterritorial impact of the GDPR on data protection laws in other jurisdictions is another category which scholars have given more consideration. Bradford describes the extraterritoriality of European laws as an attempt by the EU to influence global regulatory

---

[36] Juliane Kokott, & Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR" (2013) 3:4 International Data Privacy Law 222-228 at 222.

[37] Cara Mannion, "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets" (2020) 53:2 Vanderbilt Journal of Transnational Law 685-711 at 686.

[38] Tiffany Curtiss, "Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies" (2016) 12:1 Washington Journal of Law, Technology & Arts 96-122 at 108.

[39] Alex Makulilo, "Data Protection Regimes in Africa: Too Far from the European Adequacy' Standard?" (2013) 3:1 International Data Privacy Law 42-50 at 49.

standards through its combination of market influence and regulations, which allow the EU to set stringent regulatory standards for countries all over the world.[40] Other countries are compelled to adopt these standards, as maintaining regulatory standards lower than those set by the EU is neither economically nor legally feasible, resulting in the "Europeanization" of legal frameworks in both developed and developing countries. Mannion however asserts that the one-size-fits-all approach of European data protection regulations ignores the diverse cultural, political, and economic realities that exist in countries outside the EU and maintains that this can be classified as data imperialism.[41]

Notably in Nigeria, European data protection regulations pose significant concerns as to how the data protection framework will evolve in the future. This is because an inadequate data protection framework may create restrictions for organizations within its jurisdiction who require the transfer of personal data across borders. I argue that contemporary research on informational privacy laws in Nigeria has mainly focused on data protection as a digital right. More recently scholars such as Babalola and Salami have undertaken research on data protection laws in Nigeria, specifically taking into consideration the influence of the GDPR.[42] However, these studies have focused on the issuance of the NDPR and other data protection legislations, which only provide a limited form of compliance with the adequacy standards that requires a much broader evaluation of the data protection framework in such a country.

Although Nigeria is unlikely to seek an adequacy decision in the nearest future, the GDPR standards of "adequate protection" criterion can be used as a benchmark to holistically assess the current state of data protection. Therefore, this study aims to contribute to the existing literature

[40] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (, New York, NY: Oxford University Press 2020) at 25.
[41] Mannion, *supra* note 37 at 705.
[42] Babalola, note 35 *supra* at 1-9. See also Salami, *supra* note 28 at 576.

by assessing the Nigerian data protection framework taking into consideration the existence of data protection legislation and other factors specified in Article 45(2) of the GDPR. This dissertation also hopes to contribute by providing recommendations that, if implemented by regulators, will ensure that data protection in Nigeria receives the attention it deserves and provide a regulatory framework that is comparable with international standards.

1.3 Research Questions

This dissertation primarily aims to evaluate how "adequate" the Nigerian data protection regulatory framework is in relation to the criteria established by Article 45(2) of the GDPR, which regulate the transborder flow of personal data. While Nigeria has not requested an adequacy decision, this dissertation identifies the challenges that Nigeria will most likely face if they apply for an adequacy assessment under the standards established by the GDPR. The specific research questions are:

1. What role does the "adequate protection" criteria provided in Section 45(2) of the GDPR play in establishing an international framework for personal data protection?
2. How "adequate" is Nigeria's data protection framework in comparison with the adequacy assessment criteria provided by Section 45(2) of the GDPR?
3. What can Nigeria learn from Canada in terms of developing a data protection framework that is deemed "adequate"?

1.4 Research Methodology

In addressing the research questions, different research methodologies will be utilized. The legal doctrinal research methodology, which focuses on existing case-law on data protection, legislation, and other legal sources, in the EU, Nigeria and Canada will be the foundational basis for this research. This will be utilized to establish the role the adequacy standards in Article 45(2) of the GDPR play in creating an international data framework. The fact that the EU's GDPR is the

de facto international standard adds a political and economic dimension to this research, requiring an interdisciplinary approach. As a result, a socio-legal research method that primarily employs social-theoretical analysis is required.[43]

In analyzing how adequate the Nigerian data protection regulatory framework is in comparison with the adequacy standards of the GDPR, the research method adopted will be legal -doctrinal and comparative. This will involve a review of legal instruments, such as domesticated legislation focused on informational privacy, and other privacy-related laws in Nigeria.[44] A comparative analysis will focus on how the Nigerian statutory and regulatory framework conforms with the standards set. There will also be an analysis of case laws directly and indirectly related to the subject.[45] Reference will also be made to secondary data sources that provide an analytical means to address this question. These secondary data sources include relevant journals, newspaper publications, articles, studies, unpublished dissertations, and books.

To analyze what innovative approaches can be adopted from the Canadian data protection framework, the comparative method of research is essential. In a comparative research study of this kind, the comparative jurisdiction is an important consideration. Nigeria and Canada are both Commonwealth countries that follow the common law system and operate a federal system of government that is similar in various respects. Being one of 12 countries that have obtained adequacy decisions, a comparative analysis will also show how Canada's regulatory framework differs from that of Nigeria and what lessons can be obtained from the Canadian approach to personal data protection.

[43] This will mainly focus on articles published in socio-legal journals that address the subject.

[44] The legal doctrinal method will be used to provide an assessment of Nigeria's data privacy framework, with a focus on the NDPR and the provisions of international legislation on data privacy.

[45] Convention on the Protection of Individuals with Respect to Automatic Processing of Personal Data, 28 January 1981, ETS 108 (Entered into force 1 October 1985).

1.5 Scope and limitation of the study

The purpose of this dissertation is to see how adequate Nigeria's data protection mechanisms are in contrast with international standards which are represented by the provisions in Article 45(2) of the GDPR. The research will be limited to the concept of informational privacy, which is a subset of the broader right to privacy. The notion that "the protection of personal data is a fundamental right" has served as the foundation for a modern international approach to privacy.[46] However, transborder data flows have political and economic implications, so I focus more on the importance of an adequacy decision in the development data protection framework in this dissertation rather than establishing the concept of data protection as a human right.

In establishing an adequate data protection framework, this dissertation builds on the provisions of Article 45 and specifically sub-article 2 which creates three distinct evaluation criteria. There are exceptions to the restrictions on the international transfer of personal data, as provided in Articles 46-49. These include the use of appropriate safeguards by the data controller; binding corporate rules which are internal codes of conduct adopted by multinational groups and allow transfers between different entities; and standard contractual clauses adopted by the European Commission. It should be noted that these exceptions have lessened the impact of a country's inability to obtain adequacy decisions; however, this study limits its focus to the provisions of Article 45(2) as a benchmark in identifying international standards and does not take a comprehensive look at the state of international data transfers and the mechanisms in place to support them.

Furthermore, it should be highlighted that an in-depth analysis of the GDPR or NDPR is sufficient to cover a research paper, thus this dissertation will examine both legislations on a macro

[46] Martin Schenin, "Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism" (28 December 2009), Online: ohchr.org <https://www.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> [https://perma.cc/QWJ8-2PYL].

level comparing the provisions in both legislations and, identifying specific areas where the NDPR can be improved upon.

1.6 Terminological clarification

Certain terminology will be used throughout this dissertation that is not necessarily confined to the subject of this study and may have many definitions; consequently, it is critical to explain the context in which they are used to aid comprehension. These terms include "data protection", "transborder data flow", "adequate protection" and "third country".

1.6.1 Data Protection

The terms "data privacy", "informational privacy", and "data protection" are used interchangeably and in certain contexts may have different meanings, however, at their core, they all refer to the same principles. De Hert and Gutwirth, define data protection as a catch-all term for a range of notions about the processing of personal data, which is not possible to summarize in a few words.[47] Abdulrauf acknowledges that the term used varies depending on the jurisdiction; however, he notes that data privacy has become more widely used in the research literature by scholars in the domain.[48]

Data Protection in this context is therefore distinguishable from other subsets of the right to privacy and is built upon the definition of personal data, which the GDPR and NDPR defines as any information which is related to an identified or identifiable natural person. In general, data protection aims to protect people from the risks associated with the "processing" of their data and the different mechanisms in place to ensure such protection.[49]

---

[47] Paul De Hert & Serge Gutwirth, *"Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action"* (Dordrecht: Netherlands, Springer 2009) at 3.

[48] Lukman Abdulrauf, *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* (PHD Dissertation, University of Pretoria, 2015) [Unpublished].

[49] GDPR, *supra* note 8 at Art. 4 (1). The GDPR defines 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. See also NDPR, *supra* note 13 at Art 1.3(XIX).

1.6.2 Transborder data flows

Many legal and regulatory issues arise when personal data is transferred from one jurisdiction to another, and this is often regulated by data security and privacy legislation. This movement can be referred to by a variety of terms such as "cross-border data flow" and "International data transfers". However, there is little clarity on what the word means, with various regulatory instruments using different terminologies without specifying what they mean.[50] For the purpose of the dissertation, it will be referred to as "transborder data flows" which is the term used in the OECD guidelines and is defined as the "movements of personal data across national borders".[51]

1.6.3 Third Country

The term "third countries" is not defined in the GDPR, but it is used to refer to countries that are not signatories to the EU's primary treaties.[52] The EU law refers to any country that is not a member of the organization that is to be held accountable under that law, in this regard the GDPR applies as law to the EU and EEA, and the term 'third country' therefore refers to countries that are not EU or EEA Member States. Based on Article 45 of the GDPR, the European Commission has the authority to decide if a country outside the EU has an appropriate standard of data protection, resulting in the free flow of personal data from the EU and EEA area to that third country without the need for additional safeguards. So far, Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and most recently the United Kingdom have been recognized by the European Commission as providing "adequate protection".[53]

---

[50] Kuner, *supra* note 1 at 11.

[51] OECD Guidelines, supra note at para. 1(c).

[52] GDPR Info, Third countries, (10 April 2021), online: GDPR Info https://gdpr-info.eu/issues/third-countries/ [https://perma.cc/FM4S-D6PQ].

[53] Adequacy decisions, *supra* note 10.

1.6.4 Adequate Protection

A lack of harmonization of the divergent regulatory models available internationally led to calls for a global legal instrument on data protection. The void created by the lack of a global structure, on the other hand, has enabled the GDPR to provide international data protection standards. The GDPR's regulations strike a balance between the need for data transfers as a foundation for international business and trade, and the need to protect the fundamental right to privacy of data subjects within its jurisdiction.[54]

While this regulation establishes the free flow of personal data between Member States that are bound by the same level of protection, personal data can only be transferred outside of the EU if the GDPR's conditions for such transfers are met. This involves a two-stage process, where firstly, the processing of personal data must comply with the conditions for lawful processing stipulated in the regulation.[55] Secondly, such transfer can only be done where the European Commission determines that the "third country" obtaining this data has an adequate level of protection similar to the GDPR. The GDPR's extraterritoriality is thus a central feature of this dissertation

1.7 Research Structure

The second chapter is broken into three parts. The first part provides an overview of the global data protection framework, following its evolution from an international agreement to the GDPR. The second part of this chapter delves into an in-depth analysis of the GDPR's "adequate protection" requirements, while the third part examines current debates about the European Union's role in developing an international data protection framework.

[54] Wagner, *supra* note 26 at 320.

[55] GDPR, *supra* note 8 at art.6.

The third chapter builds on the foundations laid out in Chapter 2 by providing an overview of Nigeria's data protection framework and an assessment of its compliance with the GDPR's "adequate protection" requirement. This assessment is primarily focused on the three broad parameters outlined in Article 45 (2).

Chapter four examines the Canadian data protection regulatory framework which has received a positive adequacy decision from the European Commission. This chapter evaluates the Canadian data protection framework's compliance with the adequacy standards established under Article 45(2) of the GDPR, as well as providing a comparison with the Nigerian framework and identifying any disparities that may exist.

The fifth chapter identifies the key findings I made in this dissertation, as well as recommendations which, if adopted, can enable Nigerian regulators to adjust their approach in developing a holistic data protection framework that includes regulatory and structural improvements. I conclude by emphasizing the importance of Nigeria establishing a data protection framework that is considered "adequate".

CHAPTER 2: THE INTERNATIONAL DATA PROTECTION FRAMEWORK

2.0 Evolution of an International Framework for the Regulation of Transborder Data Flows

Transborder data flows have traditionally received little attention in public international law, with the focus instead on the general right to privacy enshrined in human rights treaties such as the Universal Declaration of Human Rights (UDHR)[56] and the International Covenant on Civil and Political Rights (ICCPR).[57] Despite the fact that these treaties do not directly reference data protection, they have served as the basis for the enactment of data protection laws in various jurisdictions.[58] Bygrave highlights that, while there is no fully global data protection framework, efforts to develop international standards have been done primarily at a regional level and, as a result, have limited international appeal.[59] This deficiency prompted the International Conference of Data Protection and Privacy Commissioners and other non-state parties to advocate for the establishment of a legally binding international framework.[60] There have also been numerous efforts to achieve this goal, including requesting a United Nations (UN) convention.[61]

The existence of an international data protection framework has been considered necessary in order to establish a strong legal foundation for shaping responses to the numerous challenges arising in the digital age, such as a lack of harmonized standards, which creates risks for the processing of personal data, and disparities in data privacy laws across different jurisdictions. This impedes global data transfer and creates significant compliance burdens and trade uncertainties.[62]

---

[56] United Nations (U.N.) General Assembly resolution 217 A (III) of 10th Dec. 1948.

[57] U.N. General Assembly resolution 2200A (XXI) of 16th Dec. 1966; in force 23rd March 1976.

[58] Christopher Kuner, "An International Legal Framework for Data Protection: Issues and Prospects" (2009) 25:4 The Computer Law and Security Report 307-317 at 309.

[59] Lee Bygrave, "Privacy Protection in a Global Context—A Comparative Overview" (2004) 47:1 Scandinavian Studies in Law 319-348 at 333.

[60] Kuner, *supra* note 58 at 307.

[61] Global Privacy Assembly, "Montreux Declaration-The protection of personal data and privacy in a globalized world: a universal right respecting diversities" (2005), online (pdf): <https://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf> [https://perma.cc/YN25-XQGU].

[62] Kuner, *supra* note 58 at 308.

Minimum standards for the processing of personal data by states, businesses, and other private actors have always been recognized as necessary. However, the establishment of these standards has resulted in regulatory models that differ across regions and nations.[63] Historically, these models have revolved around three interoperable international frameworks: the Council of Europe, the Organization for Economic Cooperation and Development (OECD), and the European Union (EU).[64] Over the last two decades, many policy actors in the international community have seamlessly transitioned from one regulatory model to the next while also attempting to domesticate or replicate these frameworks.[65] Bennett & Raab also note that two new domains in personal data protection policy have emerged in recent years: one involving standards-setting and certification, and the other impacted mostly by international political considerations and trade negotiations.[66]

The OECD Privacy Guidelines represented one of the earliest attempts to address transborder data flows from a global level. The Guidelines, which were adopted in 1980, are a non-binding set of principles that member countries may implement with the dual goal of achieving acceptance of certain minimum privacy and personal data protection standards, as well as removing, as far as possible, factors that might induce countries to limit transborder data flows.[67] The Guidelines state that member countries must recognize the consequences of domestic processing and re-exporting personal data for other member countries in their legislation.[68] Member countries must also take reasonable and effective measures to ensure that transborder data flows, including data transits, are uninterrupted and secure.[69] Membership in the OECD cuts across

63 *Ibid* at 309.
64 Colin Bennett & Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (New York, NY: Routledge, 2018) at 71.
65 *Ibid.*
66 *Ibid*.
67 Kuner, *supra* note 1 at 35.
68 *Ibid.*
69 *Ibid*.

various regions including EU Member States, countries from North America, the Asia-Pacific region, Latin America and South Africa, giving its approach to data protection a significant global reach.[70] Kirby however recognizes the OECD's limitations, due to the fact that its membership is dominated by industrialized and wealthy countries, who have contributed to the development of the guidelines and continue to influence the creation of data protection frameworks in developing countries while failing to reflect the specific data protection concerns of people living in such countries.[71]

The OECD Guidelines established a global approach to data protection but was more focused on transborder data flow regulations for commercial purposes than with enhancing privacy rights and is also non-binding from a legal perspective.[72] Convention 108 differs in this regard because it was the first multilateral treaty specifically dealing with data protection that had legally binding obligations outlined in its provisions, and it was a significant milestone in the evolution of data protection as a fundamental right.[73] The Convention requires that parties must take the necessary steps in their domestic legislation to apply the principles laid down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to personal data processing. Convention 108 is open to accession by both member and non-member states, and currently, all member states have ratified the treaty, while eight non-member states, including Senegal, Morocco, Tunisia, Cabo Verde, and Mauritius, have also acceded to it.

Significant steps were taken to avoid an unnecessary divergence between the OECD and Convention 108. They both include the fundamental principles of data protection, albeit in slightly

---

[70] *Ibid.*

[71] Michael Kirby, "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy" (2011) 1:1 International Data Privacy Law 6-14 at 13.

[72] Frits Hondius, "A Decade of International Data Protection" (2009) 30:2 Netherlands International Law Review 103-128 at 106.

[73] Kuner, *supra* note 1 at 37.

different wording and with varying degrees of articulation, and have served as models for the development of national legislation in several countries, regional agreements, and voluntary codes of practice.[74] These include data protection regulations developed in the EU based on OECD and COE principles that provide stringent regulations for the transfer of personal data outside Europe, data protection laws in Canada,[75] as well as standards formally endorsed by numerous US companies and trade associations.[76]

Other major standards that have been developed internationally include the Asia-Pacific Economic Cooperation (APEC) Privacy Framework which provides a voluntary collection of principles based on the concept of "accountability" to secure personal data transmitted outside of APEC member states.[77] This initiative aimed to facilitate transnational mutual recognition by creating a system of Cross Border Privacy Rules (CBPR) and gave countries considerable flexibility in its implementation taking into consideration their social, cultural, and other differences.[78] In Africa, the African Union convention on cybersecurity and data protection provides a comprehensive framework for data protection on the continent,[79] while regional agreements such as the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection, include provisions on the restriction of data flows.[80]

Over 145 countries have now adopted data protection or privacy laws that explicitly regulate transborder data flows.[81] However, despite the fact that most data protection laws rely on

---

74 Bennett & Raab, *supra* note 64 at 75.

75 In Canada, the Guidelines formed the basis for the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96) which has been incorporated into Canadian legislation as Schedule 1 to the Personal Information Protection and Electronic Documents Act of 2000.

76 Bygrave, *supra* note 59 at 335.

77 APEC, Digital Economy Steering Group Privacy Framework, APEC#217-CT-01.9 (2015).

78 Kuner, *supra* note 1 at 50.

79 Convention on Cyber Security and Personal Data Protection, African Union, June 27, 2014.

80 Supplementary Act on Personal Data Protection within ECOWAS, 16th February 2010, A/SA.1/01/10.

81 Graham Greenleaf, "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance" (2021) 169:1 Privacy Laws & Business International Report 3-5 at 3.

similar international standards, there exists a substantial difference across regions and legal systems.[82] While data protection laws enacted at the national level have a direct effect on individuals and provide a legal basis for individuals to exercise their rights, the present international framework only applies at a restricted level between members of intergovernmental organizations or is not legally enforceable. The lack of harmonization of the various regulatory models available internationally has led to repeated calls for a global legal instrument on data protection, and this void created has provided an opportunity for European standards, through its data protection regulations, to be exported globally as an international data protection framework.[83]

2.1 EU Privacy Regulations as An International Standard

The GDPR signified an evolution of European data protection standards that began with the implementation of the Data Protection Directive in 1995.[84] Prior to the introduction of Directive 95/46, the protection of privacy as a fundamental human right was enshrined in a number of regulations made at the national level among European countries.[85] However, there was little harmonization between these rules, as some Member States applied stricter limitations and procedures, while others had none.[86] The dependence on national data protection laws resulted in a wide range of protection levels and could not offer legal certainty.[87] Directive 95/46 was therefore proposed as a way to harmonize the rights of data subjects, as well as to unify the disparate data protection laws in its member states.[88]

---

[82] Kuner, *supra* note 1 at 159.
[83] Wagner, *supra* note 26 at 319.
[84] Paul Voigt & Axel von dem Bussche, *The Eu General Data Protection Regulation* (New York, NY: Springer 2017) at 1.
[85] *Ibid.*
[86] *Ibid.*
[87] *Ibid* at 2.
[88] *Ibid* at 2.

By regulating the processing of personal data, the purpose of harmonized European standards was to prevent the exploitation of the personal data of EU data subjects while also ensuring the unencumbered movement of data between Member States.[89] While Directive 95/46 was pioneering at the time and was intended to account for future technology growth, the rapid pace of digital innovation after more than a decade rendered it outdated in many ways when it came to dealing with modern privacy challenges.[90] For example, there were no specific requirements in the Directive for organizations to implement data protection measures for initiatives that used a large amount of personal data. Additionally, being a Directive, there were certain limitations, as it specified minimum standards and needed Member States to create their own legislation to fulfill those standards, whereas a regulation exists in its own right, superseding any applicable laws passed by Member States.[91] The GDPR was proposed in response to the need to address the gaps in the data protection regulatory framework at the time, as well as the increased significance of privacy standards in other jurisdictions.[92]

In 2011 the European Commission recommended a holistic reform of the privacy laws in the EU citing the need to adopt "a comprehensive approach on personal data protection".[93] This culminated in the drafting of a proposed regulation with the overarching goal of ensuring that European laws were relevant for the networked digital economy, establishing a uniform set of rules to provide enhanced citizen protection, and encouraging innovation in the European Single Market.[94] The GDPR was adopted on 14 April 2016 and became enforceable on 25 May 2018.

---

89 GDPR, *supra* note 8 at rec.9.

90 Voigt & von dem Bussche, *supra* note 84 at 2.

91 *Ibid.*

92 Colin Bennett, "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?" (2018) 23:2 Information Polity 239-246 at 240.

93 EDPS, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", (2011) OJ, C 181/01.

94 Bennett, *supra* note 92 at 240.

requiring compliance from organizations and persons within its regulatory purview.[95] In this regard, a number of data subjects' rights, as well as responsibilities of data controllers and processors have been established.

Although the scope of this study does not allow for a comprehensive examination of personal data rights as defined by the GDPR, the key data protection advancements and elements will be examined.

2.2 Scope of the GDPR

The GDPR was considered groundbreaking in that it established an approach to data protection that improved upon existing legislations and international guidelines in a number of ways. The regulation builds on previously established data protection principles and is hinged on seven core personal data processing principles, which include: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and accountability.[96] The regulation also broadens the definitions of personal data to include any data that can be used to directly or indirectly identify a living person and expands this to include online identifiers such as cookies and IP addresses, where they can be used for the purpose of tracking user behavior.[97] It also restricts the processing of certain categories of data, including sensitive and genetic data except when certain conditions are fulfilled.[98]

A major precondition for the lawful processing of personal data under the GDPR is that it must be based on one of the grounds listed under Article 6 which includes; the consent of the data subject; being necessary for the performance of a contract with the data subject; being necessary for compliance with a legal obligation; being necessary to protect the vital interests of the data

[95] The GDPR is directly binding and applicable because it is a regulation rather than a directive, but it does allow individual member states to adjust certain aspects of the regulation.
[96] GDPR, *supra* note 8 at art. 5 (a), (b), (c), (d), (e), (f).
[97] *Ibid* at art.4(1).
[98] *Ibid* at art.9(1).

subject; being necessary for the performance of a task carried out in the public interests; or necessary for the purposes of legitimate interests.[99] When processing is based on consent, the controller must be able to show that the data subject has given his or her consent to the processing of personal data, and where such consent is given as part of a written declaration that includes other information, the request for consent must be presented in a way that is clearly distinguished from the other information, in an intelligible and easily accessible format, and in plain language.[100] The right of data subjects to withdraw their consent at any time, subject to existing contractual obligations was also reaffirmed under the regulation.[101]

The novel and, in some cases, contentious provisions introduced is a key feature of the regulation. This includes the introduction of the right to "data portability", which allows data subjects to request information be transferred in a structured and machine-readable format from one controller to another.[102] This aims to promote the use of compatible formats and systems among processors and controllers.[103] The regulation also incorporates the "right to be forgotten", established by the Court of Justice of the European Union (CJEU) in the controversial *Google Spain* case.[104] This offers data subjects the right to request the erasure of personal data from the controller without undue delay, subject to particular conditions.[105] The GDPR also encourages the use of "pseudonymization" which ensures that personal data cannot be attributed to a data subject without the addition of other information[106] and also provides restrictions on profiling and

[99] *Ibid* art.6 a-f.
[100] *Ibid* at art.7(2).
[101] *Ibid* at art. 7(3).
[102] *Ibid* at art. 20(1).
[103] *Ibid* at rec. 68.
[104] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, (2014) ECR I-1 at I-21.
[105] GDPR, *supra* at note 8 at Art 17(1).
[106] *Ibid* at art.32(1)(a).

automated decision-making where such decisions will have a significant effect on the data subject.[107]

The GDPR's impact on privacy compliance generally is also significant as it aims to influence organizations to adopt new data protection practices. The regulation stipulates that privacy-related interests be reflected throughout the development process of information systems, and that essential data protection principles be incorporated by default into the design and development of such systems that process personal data.[108] The regulation also provides that organizations must keep a record of processing activities[109] and conduct impact assessments when utilizing new technologies to process personal data.[110] Article 37 also mandates the appointment of a data protection officer by organizations that process personal data.[111]

In order to achieve effective protection of personal data across the EU, the EU Commission considered it necessary to increase the powers of supervisory authorities for monitoring and enforcing compliance, as well as to introduce more significant sanctions for infringements.[112] One of these powers is the authority to impose administrative fines; as a result, the maximum sum an organization can be fined for violating its rules has raised to EUR 20,000,000.00, or 4% of total global turnover.[113] Recently, supervisory authorities have imposed administrative penalties on international technology giants such as Amazon and Google for data breaches.[114] In addition to administrative penalties, organizations may be required to compensate data subjects.[115] In this

---

[107] *Ibid* at art.22 (1).
[108] *Ibid* at art.25 (1).
[109] *Ibid* at art.30 (1) (2).
[110] *Ibid* at art.35 (1).
[111] *Ibid* at art.37 (1).
[112] *Ibid* at rec.11.
[113] *Ibid* at art.83 (5).
[114] Software world, "Number of GDPR Fines Surge by 113% in a Year despite Strict Regulations" (October 3, 2021), Online: Software World https://link.gale.com/apps/doc/A674513635/ITBC?u=uvictoria&sid=summon&xid=102f8cb8 [Permalink: https://go.exlibris.link/JFL92XC8].
[115] GDPR, *supra* note 8 at art.82(1).

regard, it is noteworthy that, for the first time, the regulation expanded the scope of liability, as organizations could be held civilly liable for GDPR violations.[116]

2.3 The extraterritorial application of EU Regulations

In terms of its territorial reach, the regulation applies to all firms that offer products and services to EU residents, regardless of whether they are based inside or outside the EU.[117] It also applies to all companies processing the personal data of EU residents, regardless of where they offer products or services to them or whether their personal data is processed manually or automatically.[118] In effect, to ensure that the rights of individuals are not infringed, this expanded territorial scope introduced the principle of *lex loci solutionis*, which states that the applicable law is determined by the location of the relevant contractual performance.[119] The exercise of this expanded territorial scope has had consequences for multinational corporations, governments, and users, revolutionizing data protection laws around the world as well as changes in data protection procedures of international and non-EU corporations.[120]

This is essentially a unilateral extension of European law to non-EU organizations, with the internet's global scope necessitating the implementation of data protection laws across borders serving as a major justification. The decision in the *Google Spain* case, in which the CJEU was asked to rule on the applicability of EU data protection law to a data controller based in a third country, also solidified the position that the data protection regulations in the EU apply extraterritorially.[121] In reaching its decision, the Court held that Google Inc. the parent company of the Google Group, which had its seat in the United States and exploited the search engine

---

[116] Voigt & von dem Bussche, *supra* note 84 at 21.
[117] GDPR, *supra* note 8 at art.3(2).
[118] Voigt & von dem Bussche, *supra* note 84 at 26.
[119] *Ibid*.
[120] *Ibid*.
[121] *Google Spain*, supra note 104 at para 60.

Google Search, was considered the data controller and its subsidiary, Google Spain, the establishment. The court clarified that EU data protection laws may apply even if the principal establishment is located outside of the EU or in a third country.[122]

With respect to the legal basis of the extraterritorial application of the GDPR, The Article 29 Working Party (WP 29) has held that transborder jurisdictional issues in data protection law are generally a question of international law.[123] The territoriality principle which stipulates that jurisdiction is based on activities undertaken within the territory of the state in issue is considered to be the foundational basis of legitimacy.[124] However, the internet complicates the application of the territoriality principle, as it can be difficult to pinpoint an online action as occurring in a specific state.[125] Azzi argues that article 3(2) of the GDPR appears to be founded on the "effects doctrine" which is a controversial basis of jurisdiction because it is defined on the basis that activity that occurs outside the state has effects within the state.[126] In essence, the GDPR places the focus on the location of the potentially harmful effects and discards the location of the processing of the operator.[127] However, as Kuner points out, this also poses some difficulty as it is open-ended, especially in a globalized economy where "everything has an effect on everything".[128]

Extraterritoriality of regulations presents some obvious challenges in enforcement where such organizations are not registered within jurisdiction, and the EU legislator, in an effort to

[122] Paul de Hert & Michał Czerniawski, "Expanding the European data protection scope beyond territory: Article 3 of the general data protection regulation in its wider context" (2016) 6:3 International Data Privacy Law 230-243 at 233.
[123] WP 29, Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (2002) OJ, C 5035/01.
[124] Adele Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation" (2018) 9:2 Journal of Intellectual Property, Information Technology and E-Commerce Law 126-137 at 130.
[125] Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)" (2010) 18:2 International Journal of Law and Information Technology 176-193 at 188.
[126] Azzi, *supra* note 124 at 130.
[127] *Ibid.*
[128] Kuner, *supra* note 125 at 190.

circumvent this, introduced the role of representatives.[129] This necessitates that any organization which is subject to Article 3(2) and does not have an establishment in the EU shall designate a representative in the EU, such organization may only designate one representative, a legal entity or an individual for the whole territory of the EU.[130] The primary role of the representative is to represent foreign operators with regard to their obligations and create a legal nexus between them and the EU authorities.[131] More specifically, the representative is required to cooperate with the authorities regarding any action ordered to ensure compliance with the regulation.[132] The designation of a representative does not affect the responsibility or liability of the operator, but such a representative may be subject to enforcement proceedings in the event of non-compliance by the controller or processor.[133]

2.4 Data Transfer Mechanisms Under the GDPR

In conformity with previously established standards under Directive 95/46, the GDPR retained provisions restricting the export of personal data of EU data subjects except where specified mechanisms outlined in the regulation were put in place. The data transfer mechanisms establish an additional layer of extraterritoriality that complements the provisions of Article 3(2) of the GDPR. While both provisions are concerned with the processing of data of EU subjects within its territory, they are directed at different players. Art. 3(2) targets non-EU legal entities that process personal data or monitor data subjects' behavior and compels compliance with the regulation, while Art. 45 imposes restrictions on EU operators, forbidding them from transmitting

[129] GDPR, *supra* note 8 at art.27(1).
[130] *Ibid* at rec 80.
[131] Azzi, *supra* note 124 at 133.
[132] GDPR, *supra* note 8 at art.31.
[133] *Ibid* at rec 80.

personal data to third-party parties that do not meet the criteria provided under Article 45(2) of the regulation.[134]

The GDPR also provides that the transfer of personal data to a third country or an international organization from the EU can only take place if the controller and processor comply with the conditions outlined in Articles 45-49 of the regulation.[135] In this context, firstly, data exporters need to fulfill all the obligations for personal data processing under the GDPR, which include implementing the basic data protection principles and be grounded on a lawful basis for processing.[136] Secondly, a data exporter must then observe the specific rules which require that data exporters choose one of the different transfer mechanisms available under the regulation and ensure that a high level of protection of fundamental rights is maintained.[137]

The GDPR provides a multi-tiered framework, creating three channels for international data transfers. Although the GDPR uses different expressions to describe the standard(s) of protection required for international transfers of data, the one that recurs most often is the "adequate level of protection". This first tier establishes parameters under which the Commission makes decisions on a third country's level of adequacy, and where determined, data transfers from the EU can take place without restrictions.[138] The second tier establishes legal justifications for data transfers subject to "appropriate safeguards", in which controllers and processors exporting personal data give guarantees for third-country controllers or processors, this includes the use of standard contractual clauses drafted by the commission,[139] binding corporate rules,[140] and an

134 Voigt & von dem Bussche, *supra* note 84 at 117.
135 GDPR, *supra* note 8 at art. 44.
136 Ibid at art.6.
137 Zuzanna Gulczyńska, "A Certain Standard of Protection for International Transfers of Personal Data Under the GDPR" (2021) International Data Privacy Law 360-374 at 360.
138 *Ibid*.
139 GDPR, *supra* note 8 at art. 46(1) & (2).
140 *Ibid* at art. 47(1).

approved code of conduct subject to Article 40 of the GDPR.[141] Thirdly, in the absence of an adequacy decision and transfers subject to appropriate safeguards, transfers can only take place when specific requirements classified as a list of derogations are met.[142]

The GDPR does not establish a formal hierarchy among the data transfer mechanisms available, but it is clear from the wordings of its articles that there is some form of order. Article 46(1), for example, states that the controller or processor may in the absence of a decision pursuant to Article 45(3), "transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available".[143] Article 49(1) also provides that in the absence of an adequacy decision, or of appropriate safeguards pursuant then the list of derogations may be utilized. This implies that adequacy decisions are prioritized as a data transfer mechanism before other transborder data transfer measures are considered.

In this regard, the significance of the GDPR's adequacy protection provisions as they relate to transborder data transfers is well established. As a result, the criteria outlined in Article 45(2) serve as a suitable reference point for assessing data protection standards in third countries.

2.5 The GDPR's Adequacy Protection Provisions

Analyzing the provisions of Article 45(1) of the GDPR which affirms that transfers to third countries must be based on an adequacy decision, is central to this dissertation in terms of the impact of the regulation on international data privacy. Article 45(1) provides that personal data can only be transferred to a third country or an international organization if the European Commission has determined that the third country provides an "adequate level of protection".[144]

---

[141] *Ibid* at art. 46(2) (e).
[142] *Ibid* at art. 49(1).
[143] *Ibid* at art. 46(1).
[144] *Ibid* at art. 45(1).

The GDPR provides that the commission has the sole responsibility for determining adequacy and where there is a positive decision, data exporters do not need to take any additional steps besides verifying that adequacy decisions apply to their transfers.[145] Overall, this aims to promote certainty and uniformity of data privacy protection frameworks across various jurisdictions.[146]

The framework for evaluating the adequacy of a third country's protection framework is in Article. 45(2), which outlines the elements to be taken into consideration by the European Commission when assessing adequacy. For this assessment, the most important elements are broken down into three criteria, which are:

1.First Criteria: this criteria is considerably broad, however the identified elements are, the rule of law and respect for human rights and fundamental freedoms; Legislation related to public security, defence, national security and criminal law and the access of public authorities to personal data; specific data protection legislation including rules for the onward transfer of personal data to another third country; enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.

2.Second criteria: this considers the existence and functionality of an independent supervisory authority in the third country with responsibility for ensuring and enforcing compliance with data protection rules.

3.Third criteria: this considers the international commitments or other obligations the third country concerned has entered into in relation to the protection of personal data.

In the case of third countries that have already received a positive adequacy assessment, a "sunset clause" is included, which requires the Commission to keep an eye on developments in that country that may have an impact on the operation of data transfers based on those decisions,

[145] *Ibid* at art. 45(3).
[146] *Ibid* at rec. 103.

as well as a periodic review, at least every four years.[147] Article 44(9) GDPR also allows Member States a four-year transitional period during which adequacy decisions made under Directive 95/46 remain in effect.[148] Therefore, the Commission will soon assess whether prior adequacy decisions made under Directive 95/46 will continue to apply under the GDPR.

2.6 An Examination of the Substantive Requirements for Assessing Adequacy

The GDPR does not give a specific definition of what constitutes an adequate level of protection. Therefore, reference must first be made to the provisions of Article 45(2) which provides some guidance as to what elements are considered in assessing adequacy. The importance of the assessment criteria is indicated in the wording of Article 45(2) which specifies that when determining adequacy, the Commission must consider the elements stipulated "in particular". This infers that although the Commission is not strictly bound by the evaluation criteria outlined, it must use it as a baseline when conducting an adequacy assessment.[149] Outlining these elements provides some structure beyond what existed under Directive 95/46, which had no framework but stated that a third country's level of protection "shall be assessed in light of all the circumstances".[150]

As previously stated, Article 45(2) contains three broad evaluation criteria, and to establish the parameters for conducting an assessment in subsequent chapters, an analysis of what each criteria entail is required to determine how adequate a third country's level of protection is.

[147] *Ibid* at art.45(3).
[148] *Ibid* at art.44(9).
[149] *Ibid* at art. 45(2).
[150] DPD, *supra* note 23 at art. 25(2).

2.6.1 First Criteria: Article 45 (2) (a): The Rule of Law, Respect for Human Rights, and Fundamental Freedoms and Enacting Relevant Legislation

Article 45(2)(a) of the GDPR sets out the legal standards that a third country must satisfy to be considered as having an adequate data protection framework. Wagner states that these criteria can be further subdivided into two components which are the general and specific components.[151] Wagner's classification process streamlines the analysis of this broad criteria, stating that the general component focuses on the presence of a regulatory framework that respects the rule of law, fundamental rights and freedoms, as well as the existing legislation in such countries in terms of public security, defence, national security, and criminal law.[152] The specific component focuses on data protection by the enactment of laws that regulate privacy to a comparable standard as the GDPR, the implementation of these laws, access of public authorities to personal data, as well as the existence of an effective redress mechanism for data subjects to exercise their rights.[153]

In assessing the requirement that third-countries adhere to the rule of law and respect for human rights and basic freedoms, the standards under EU law have been relatively well defined in Article 2 of the *Treaty on European Union* (TEU) which provides that "values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities*"* must exist.[154] Further reference is also made in the Copenhagen criteria to the "stability of institutions guaranteeing democracy, the rule of law, human rights" as a requirement as a prerequisite for a country to become a member of the EU.*[155]* This implies that third countries are obligated to adhere to the same standards in respecting the rule of law as EU member states.

---

151 Wagner, *supra* note 26 at 321.
152 *Ibid*.
153 *Ibid*.
154 EC, Consolidated Version of the Treaty on European Union, (2008) OJ L 115/13 at 17.
155 EC, Conclusions of the Presidency on the European Council in Copenhagen, (1993) C 180/93 at 13.

Fundamentally, the rule of law, as defined under EU law, requires the establishment of a system of separation of powers with political checks and balances represented in a constitutional system.[156] It further consists of the principles of legality, legal certainty, the prohibition of executive arbitrariness, independent and effective judicial review, and equality before the law.[157] The rule of law, contemplated here, underpins, supports, and ensures the practice of democracy, which goes beyond having a set process for electing a government and emphasizes the accountability of elected officials through the limitation of their power. With respect to human rights, the third country has to respect the rights acknowledged by Article 6 TEU which itself refers to the Charter of Fundamental Rights of the EU, the European Convention for the Protection of Human Rights and Fundamental Freedoms and to the fundamental rights which result from the constitutional traditions common to the EU Member States.[158]

In terms of the expected level of observance of the rule of law in third countries, Judicial decisions of the CJEU have provided some guidance by employing the principle of proportionality, mandating that legislation approved by countries do not exceed the bounds of what is "appropriate and necessary" to achieve the legitimately pursued objectives.[159] For example, in *Digital Rights Ireland v. Seitlinger*, the CJEU ruled that the EU's Data Retention Directive 2006/24, which mandates the blanket retention of data on suspicious individuals, violates the EU Charter of Fundamental Rights and exceeds the scope of what is considered a proportional and necessary means of achieving public security.[160]

---

156 Thomas Von Danwitz, "The Rule of Law in the Recent Jurisprudence of the ECJ" (2014) 37:5 Fordham International Law Journal 1311-1343 at 1334.

157 Wagner, *supra* note 26 at 322.

158 *Ibid*.

159 Von Danwitz, *supra* at note 156 at 1330.

160 *Digital Rights Ireland Ltd and Kärntner Landesregierung and Others*, C-293/12 & C-594/12, [2014] ECR at 17.

2.6.2 Specific data privacy principles: the standard of essential equivalence

The second component of Article 45 (2) (a) is specifically focused on data protection and evaluates the data protection laws and practices in effect in a third country. This necessitates the implementation of regulations that are consistent with European data protection standards, the establishment of a legal framework that protects data privacy rights, and the existence of an effective data subject redress mechanism. Determining how adequate a third country's data protection rules are, on the other hand, is not as straightforward, prompting third countries to develop GDPR-influenced legislation.[161] While Article 45 (2) (a) does not provide much guidance on what GDPR compliant legislation should include, the CJEU has expressly clarified that:

> The word adequate admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, the term "adequate level of protection" must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is "essentially equivalent" to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.[162]

The term "essentially equivalent" was also adopted as the expected standard for data protection laws by recital 104 of the GDPR and it is in this context that Article 45(2)(a) should be understood. This standard of "essential equivalence" has been primarily developed through pronouncements by the CJEU in the seminal cases now referred to as *Schrems I*[163] and *Schrems II*[164]. In *Schrems I,* the CJEU established that the "Safe Harbor Agreement", a European Commission decision that affirmed that the US protected personal data to an adequate level, was invalid. The Court agreed

---

[161] Graham Greenleaf, "Global Data Privacy Laws 2019: New Eras for International Standards" (2019) 157:1 Privacy Laws & Business International Report 1-4 at 1.

[162] *Maximillian Schrems v Data Protection Commissioner*, C-362/14, [2015] ECR at para 73.

[163] *Ibid.*

[164] *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, C-311/18 [2020] ECR.

that the Agreement did not guarantee a sufficient level of personal data protection and was anachronistic to the obligations embodied under the EU data protection laws.[165] Central to this conclusion were concerns about the indiscriminate collection and access to personal data by US intelligence agencies and the fact that the Safe Harbor principles only applied to companies that subscribed to a self-certification mechanism, failing to regulate the activities of public authorities.[166] The court also noted broader exemptions in the application of data protection principles where issues of national security, public interest, and law enforcement were concerned.[167]

In determining what the CJEU considers to be essentially equivalent, it was clarified in *Opinion 1/15*, a case involving a draft agreement between the EU and Canada on transferring passenger name record (PNR) data, that the starting point for evaluating the standard of "essential equivalence" is assessing whether there is an interference with a fundamental right protected under the EU Charter of Fundamental Rights.[168] In this context, the test must pass the Article 52(1) Charter threshold which provides that any limitations on the exercise of the rights and freedoms recognized by the EU Charter must be provided for by law and respect the essence of those rights and freedoms. Such interferences have been determined to include a breach of the fundamental rights to privacy,[169] personal data protection,[170] the right to effective judicial protection[171] and also the right to non-discrimination.[172] An assessment of an interference with fundamental rights in relation to data transfers is also subjected to a proportionality assessment, which considers whether

[165] DPD, *supra* note 23 at art 25 & 26.
[166] *Schrems I*, *supra* note 162, at paras. 88-89.
[167] *Ibid*.
[168] Opinion 1/15 Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data from the European Union to Canada [2017] OJ C 592/1 at 40.
[169] TEU, *supra* note 154 at art.7.
[170] *Ibid* at art.8.
[171] *Ibid* at art.47.
[172] *Ibid* at art.21.

such interference is necessary to achieve its objectives, and the CJEU emphasized the need for specific safeguards to ensure an appropriate balance.[173]

The CJEU continued the advancement of the standard of "essential equivalence", with regard to its scope, in *Schrems II,* which was based on the same material facts as *Schrems I* and addressed the adequacy of the "privacy shield" designed as a successor to the safe harbor agreement.[174] The CJEU once again invalidated the privacy shield and in reaching their decision emphasized that the standard of equivalence envisioned does not only cover the extent of data protection with respect to legislation but must also factor in elements such as how detailed national security laws are with respect to the collection of personal data, the ability of government agencies to access personal data, the practical nature of data protection in countries that have enacted similar laws and what mechanisms exist to enforce the rights of data subject.[175]

The CJEU also considered what level of protection is contemplated in drafting data privacy laws in third countries. An analysis of the standards as delineated in the *Schrems I* and *Schrems II* judgments' provides that this "essential equivalence" does not necessitate a replica of all of the GDPR's principles.[176] Determining which principles must be present is more complex as some provisions of the GDPR are still relatively contentious, such as the right to be forgotten as provided under Article 17, and in certain cases the application of such principles may be impractical in third countries.[177] Bennett however affirms that a starting point for assessing "essential equivalence"

---

[173] David Lindsay, *The Role of Proportionality in Assessing Trans-Atlantic Flows of Personal Data* (Antwerp, Belgium: Intersentia 2017) at 55.
[174] Schrems II, *supra* note 164 at Para 96.
[175] *Ibid.*
[176] Gulczyńska, *supra* note 137 at 14.
[177] Sara Duque de Carvalho, "Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108" (2019) 5:1 European Data Protection Law Review 54-64 at 58.

with respect to data protection laws is an incorporation of the core data subject rights on which the GDPR is hinged.[178]

2.6.3 Second Criteria: The Existence and Functioning of Independent Supervisory Authorities

The second criteria established in Article 45(2) (b) for assessing how adequate a third country's level of protection is the existence and functioning of an independent supervisory authority in the third country with responsibility for ensuring and enforcing compliance with data protection rules. The importance of independent supervisory authorities has been well established by the CJEU who have defined their role in ensuring data protection and asserting that they protect individuals' rights to personal data protection and are therefore the guardians of those fundamental rights.[179] In analyzing what is expected for an implementation of this criteria in third countries, the judicial pronouncements of the CJEU which have since been incorporated by the GDPR, provide a framework for the establishment of supervisory authorities within the EU and establish the level of independence contemplated in third countries.

The GDPR provisions with respect to the structure of supervisory authorities are considerably detailed and provide some guidance that can be adopted as a benchmark for assessing the existence of similar institutions in third countries. The regulation provides that each Member State must designate one or more independent public authorities to oversee the implementation of the regulation in order to protect natural persons' fundamental rights and freedoms in relation to processing and to allow for the free flow of personal data.[180] The CJEU has also emphasized that the conception of an independent authority is to ensure that there is an agency capable of protecting the individual rights of data subjects as well as a mechanism to effectively counter the interests of

[178] Bennett, *supra* note 92 at 243.
[179] *European Commission v Federal Republic of Germany*, C-518/07 [2010] ECR at 4.
[180] GDPR, *supra* note 8 at art.51 (1).

organizations that process personal data.[181] This level of independence also allows the supervisory authority to engage constructively with state actors and government departments in order to ensure that data protection rules are followed.[182] A robust judicial oversight is also a crucial tool for enforcing this independence, as where a supervisory authority fails to perform its function, individuals may apply to the court to compel compliance.[183]

The GDPR further provides that a supervisory authority shall act with complete independence from public and private actors in performing its tasks and exercising its powers, while its members must remain free from external influence in the performance of their tasks and exercise of their powers whether direct or indirect and shall neither seek nor take instructions from anybody.[184] In this regard it is required that a supervisory authority must be financially autonomous to ensure that their independence is not restricted by any form of control tied to funding.[185] It is further provided that they must have separate, public annual budgets, which may be part of the overall state or national budget.[186] The CJEU has further emphasized that even indirect interference, such as an unrestricted right to be informed about the supervisory authority's activity, is prohibited.[187]

The GDPR provides for the enactment of an enabling law for the establishment of the supervisory authority and incorporation of provisions that clearly stipulate the rules and procedure for appointment of members, including the qualifications expected of members, eligibility criteria and duration of tenure.[188] The GDPR unambiguously permits member states to establish an

---

[181] Felix Bieker, *Enforcing Data Protection Law – the Role of the Supervisory Authorities in Theory and Practice* (Cham, Springer International Publishing, 2017) at 126.
[182] *Ibid*.
[183] *Ibid* at 135.
[184] GDPR, *supra* note 8 at art. 52 (1) & (2).
[185] *Ibid* at art.52 (6).
[186] *Ibid*.
[187] Bieker, *supra* note 181 at 127.
[188] GDPR, *supra* note 8 at art. 54 (1).

appropriate method of appointment that represents their state's form of government, based on the provisions of the regulation. In practice, this is accomplished in a variety of ways. For example, members of the French Commission Nationale de l'Informatique et des Libertés (CNIL) are chosen from a variety of institutions, including the parliament and the courts, while in Germany the heads of the supervisory authorities are elected by the federal or regional parliaments, which may be through an instrument of parliament or in some instances through an election.[189]

While there are no clear judicial pronouncements on how compliant supervisory authorities should be with European standards, it can be inferred from the interpretation of the court in determining an adequate level of protection that the standard should be one of "essential equivalence", which indicates that third-country supervisory authorities will be expected to maintain a level of independence and have the powers established under Chapter VI of the GDPR. However, this will also be expected to reflect the system of governance and the practical realities in third countries.

2.6.4 Third Criteria: the international commitments or other obligations the third country concerned has entered into in relation to the protection of personal data

The third criteria as provided in Article 45(3) provides that the commission will consider the international commitments or other obligations the third country concerned has entered into in relation to the protection of personal data. This consideration includes participation in multilateral or regional frameworks which aim to protect personal data and regulate transborder data flows such as the OECD guidelines and Convention 108. Wagner asserts that by including this provision, the EU demonstrates its openness to public international law by explicitly referring to international treaties in an interpretation of the European data export regime.[190]

[189] Bieker, *supra* note 181 at 127.
[190] Wagner, *supra* note 26 at 32.

This provision appears to be very straightforward in its interpretation, and the CJEU reiterated in *Schrems I* that when determining adequacy, the court will consider the international commitments made by a third country.[191] While the CJEU does not specify which international commitments will be taken into account, Recital 105 provides some clarity by stating that accession to the Council of Europe Convention 108 should be specifically taken into account, however, Carvalho contends that mere accession to Convention 108 is insufficient to suggest that a country's data protection level is adequate.[192] Non-EU member states can accede to Convention 108, and while the EC maintains that an accession will be considered favorably, Argentina remains the only state to have received a positive adequacy decisions out of eight Non-EU states that have so far acceded to the Convention, which I argue significantly diminishes the significance of such an accession. However, the inference to be drawn is that the international commitments to be entered into as contemplated by this Article are those that closely mirror European standards and serve as a suitable starting point for determining adequacy.[193]

2.7 Extrinsic Considerations in determining Adequacy

The evaluation criteria of the regulation have provided some guidance and a launchpad through which the data protection framework of a third country can be evaluated. However, in practice evaluating adequacy is a complex process, with only 13 countries receiving favorable adequacy determinations. The EC does not provide detailed information on countries that have applied for adequacy, however it is noted that there have been considerable efforts from countries such as Mauritius, Morocco, and Senegal to achieve this status.[194] Despite these attempts no

[191] *Schrems I*, *supra* note 162 at para 73.
[192] Carvalho, *supra* note 177 at 56.
[193] *Ibid.*
[194] Makulilo, *supra* note 39 at 44.

African country has received a positive adequacy decision.[195] The rarity of adequacy decisions, as well as the perceived exclusion of African countries, raises the question of whether the European Commission's standards are extremely high and largely unattainable, or if considerations other than those specified in the GDPR play a role.[196] Makulilo argues that the considerations contemplated by the EC may include political and economic factors which may influence a positive or negative adequacy decision.[197]

The European Commission is the body tasked with making decisions about what constitutes an "adequate level of protection" in a third country. When exercising this function, the Commission's procedure begins with the acceptance of a draft adequacy proposal by the College of EU Commissioners, followed by a non-binding opinion from the European Data Protection Board (EDPB).[198] Article 70 of the GDPR states that the EDPB must provide the Commission with an opinion on the adequacy of a third country's level of protection, this opinion includes criticisms which in certain cases require a third country to make amendments.[199] To accomplish this, the commission must provide the board with all necessary documentation, including correspondence with the third country's government.[200] Following that, it is necessary to obtain the approval of the committee composed of representatives from EU Member States, as well as the final approval of the college of EU commissioners.[201]

While this outlined process of determining adequacy appears to be lengthy and complex, the complexity is further exacerbated by the political and technical negotiations that precede any

---

195 *Ibid* at 45.

196 *Ibid*.

197 *Ibid* at 49.

198 GDPR, *supra* note 8 at Rec 105. This was previously referred to under Directive 95/46 as the Working Party 29, (WP 29) an Independent Advisory Committee on data protection, among whose responsibilities it is to advise the Commission on the level of data protection in third countries.

199 *Ibid* at art. 70 (1) (s).

200 *Ibid*.

201 Carvalho, *supra* note 177 at 57.

EU Commission decision. These negotiations take the form of dialogues between a third country and the EU, such as the Japan-EU dialogue, which began in 2017 with the goal of establishing a framework for the mutual and smooth transfer of personal data and resulted in an adequacy decision termed the "World's Largest Area of Safe Data Flow".[202] Economic factors and political considerations have been a primary driver of such dialogue, as underscored by the European Commission, which emphasized prioritizing discussions on a potential adequacy decision with Japan, as well as other key trading partners in East and Southeast Asia.[203] This is further illustrated by the importance of the EU-Japan adequacy decision for bilateral trade, which was negotiated alongside and complemented the Economic Partnership Agreement (EPA) entered into by the two parties.[204] Given that the EU is Japan's third-largest export market, Suda argues that the importance of unrestricted data transfer for commercial reasons preceded other factors such as the protection of fundamental rights.[205]

The argument by Niebel that the GDPR's extraterritorial provisions represent the EU exerting political influence and attempting to frame various aspects of international commerce and trade is also central to this discourse.[206] This he argues is primarily accomplished through its large consumer market, consumer data access, strong political will, and enforcement mechanisms.[207] Bradford identifies this as the "Brussels effect" which is based on the concept of unilateral regulatory globalization, in which regulations become global as a result of particular economic forces. In this instance, companies must adhere to EU standards in order to gain access to the EU

202 Flora Wang, "Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement" (2020) 33:2 Harvard Journal of Law & Technology 661-690 at 671.
203 Yuko Suda, "Japan's Personal Information Protection Policy Under Pressure" (2020) 60:3 Asian survey 510-533 at 521.
204 *Ibid*.
205 *Ibid* at 523.
206 Crispin Niebel, "The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy" (2021) 40:4 The Computer Law and Security Report 1 -15 at 1.
207 Bradford, *supra* note 40 at 25.

market.[208] Kuner asserts that one method used to achieve this is the "carrot and stick" approach, in which the EU dangles an offer of extending preferential status to third countries if their data protection standards are certified as being "essentially equivalent" to those of EU law, and thought to grant economic benefits by allowing personal data to be freely transferred to such countries.[209] While the "stick" allows for free flow of data to third countries only if they adopt EU standards or prohibits data transfer to such countries that are found to be inadequate.[210]

An inconsistent application of adequacy principles complicates the decision-making process for jurisdictions seeking a decision and lends credence to the argument that other extrinsic factors influence determinations by the European Commission.[211] This is most evident in the various ways in which countries can be found to satisfy the GDPR's principles despite obvious flaws in their data protection regimes.[212] The WP 29 analysis of the independence and effectiveness of Argentina and Monaco's Data Protection Authorities is an example of this inconsistency. In the case of Argentina, the WP 29 issued a favorable opinion at a time when the country's Data Protection Authority had issued no significant guidance and pursued no enforcement, limiting its analysis to the text of the law and failing to take into account other factors such as the Authority's political independence, budget, or staff selection.[213] The WP 29's Monaco Opinion, on the other hand, revealed a very different approach, where The WP 29 noted that, even under a broad interpretation of "complete independence", Monaco's Commission de Controle des Informations Nominatives (CCIN) would not be considered independent because the expenditure

---

208 *Ibid*.

209 Christopher Kuner, "The Internet and the Global Reach of EU Law" (2017) LSE Legal Studies Working Paper No. 4 at 24.

210 *Ibid.*

211 Jennifer Stoddart, Benny Chan, & Yann Joly "The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research" (2016) 44:1 Journal of Law, Medicine & Ethics 143-155 at 146.

212 *Ibid* at 147.

213 *Ibid.*

control exposes the body to the government's influence on the recruitment and promotion of staff, potentially jeopardizing its independence.[214]

The disparity in this approach reflects the discretionary nature of applying adequacy principles, as the decision in Argentina's case demonstrates that the Commission may be willing to overlook gaps in enforcement, whereas in Monaco, despite finding the data transfer practices problematic, the Commission took positive steps not only to seek clarification in the law but also to broker a deal to ensure that these practices did eventually meet its requirements. It is also noteworthy that the EU only publishes the reasons for its decisions when it makes a positive adequacy decision, not when it considers an application and comes to a negative conclusion.[215] As a result, there has been far less information available about what constitutes and does not constitute "adequacy" than would be beneficial.[216]

The unpredictability and inconsistency of adequacy assessments continue to discourage third countries and international organizations from undergoing this assessment, reducing its effectiveness as a tool in developing a functional and straightforward process for transborder data flows between the EU and third countries. Therefore, improving the transparency, accountability, and predictability of future adequacy assessments may help to reduce some of the uncertainty. A more participatory process in which third countries could engage in a dialogue on the adequacy assessment process would also be beneficial as it would help to clarify the standards to which they must adhere to achieve or maintain their adequacy status. Notwithstanding these practical deficiencies, the theoretical standards outlined in the GDPR still provide a good framework for assessing how adequate a third country's data protection framework will be evaluated to be.

---

214 *Ibid.*

215 Makulilo, *supra* note 39 at 49.

216 *Ibid*.

Chapter 3: AN EVALUATION OF THE NIGERIAN DATA PROTECTION FRAMEWORK

3.0 Introduction

I established in the preceding chapter, that the GDPR created an international standard that influenced the development of data protection frameworks in third countries such as Nigeria. Nigeria has also made significant efforts to improve its data protection framework, and in this chapter, I examine how adequate Nigeria's data protection framework is in comparison to the adequacy assessment standards established in Section 45(2) of the GDPR. To accomplish this, I begin with an overview of data protection in Nigeria, identifying previously and currently existing legal frameworks and legislative efforts to protect personal data. I then conduct an in-depth examination of Nigeria's current data protection framework's adequacy, taking into account the GDPR's three adequacy assessment criteria. Finally, based on the assessment conducted, I present my argument as to whether Nigeria's data protection framework is adequate.

3.1 The Evolution of Data Protection in Nigeria

In Nigeria, data protection is a relatively new field that has only recently received increased attention from regulators, scholars, and digital rights advocates in terms of the need to develop an effective regulatory framework. This increased importance can be attributed to a number of factors, including the progressive adoption of technology, which has impacted the public and private sector through massive efforts to digitize records containing the personal data of citizens, and significant investment in technology across major sectors that increasingly uses personal data for a variety of purposes.[217] Makulilo observed that the increased international focus on data protection, particularly with regard to transborder data flows, puts the spotlight on Nigeria to create an

[217] Lukman Abdulrauf, & Charles Fombad. "Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms" (2017) 38:2 Liverpool L Rev 105-134 at 108.

adequate data protection framework, owing to its position as one of Africa's largest economies, political significance, and population size.[218]

Historically, the communal culture of Nigeria's various ethnic groups meant that a greater emphasis was placed on social cohesion rather than individuality, and traditional Nigerian societies did not emphasize individual privacy in the same way that Western societies did, which is reflected in the development of the Nigerian data framework, which until recently showed little to no concern for enacting data protection laws.[219] As a result, the majority of the laws and regulations governing data protection in Nigeria are influenced by a western approach to data protection and have been heavily influenced by international data protection standards, most notably European regulations contained in the GDPR.[220] This approach, however, has been met with criticism, with scholars such as Iwobi emphasizing that using this mechanism of legal transplantation has been disadvantageous to the nation's search for an appropriate statutory framework.[221] This approach, he argues, has resulted in various attempts to create draft data protection legislation that reveal an alarming lack of in-depth knowledge of the transplanted laws, as well as a lack of the sophisticated mindset required to make those laws applicable to the Nigerian context.[222]

In terms of the socio-political context of data protection, Nigeria's rapid technological evolution has seen the proliferation of platforms for online shopping, online banking, e-learning, and e-government. This has also resulted in more personal data being used by organisations and the government with limited consideration of their privacy implications. Nwankwo contends that

---

[218] Alex Makulilo, "Nigeria's Data Protection Bill: Too many surprises" (2012) 120:1 Privacy Laws & Business International Report 24-27 at 25.

[219] Samuel Nwankwo, *Information Privacy in Nigeria in Alex Makulilo, African Data Privacy Laws* (Cham: Springer International Publishing, 2016), at 51.

[220] Graham Greenleaf, "Nigeria regulates Data Privacy: African and Global Significance" (2019) 158 Privacy Laws & Business International Report 1-4 at 1.

[221] Andrew Iwobi, "Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime"' (2016) 26:1 Transnational law & contemporary problems 14-59 at 15.

[222] *Ibid.*

the overwhelming nature of the applications of ICT devices and infrastructure in the early stages of their arrival made it appear unimportant to begin any meaningful discussion about whether the prerequisites for their use had been met.[223] Mannion asserts that this approach to issues such as privacy, security, data protection, and rights is common in African countries, and differs from that of the EU, where assessing the privacy impact of emerging technology is always prioritized. [224]

Nwankwo admits that Europeans may have some historical, philosophical and technological reasons for their stance on privacy, but argues that there has been a recent understanding that Nigerian data subjects face similar data protection concerns as those in Europe.[225] The challenges encountered affect both the private and public sectors as personal data exploitation by financial technology companies, particularly those offering quick loans, has been a major source of concern in the private sector. Companies have been reported to access personal contacts of customers who are not parties to the transaction in order to recover such loans.[226] Concerns have also been raised in the public sector about the overcollection of personal data by public bodies for similar purposes, as well as how this personal data is collected, stored, and used. Specific concerns include the collection of personal data for the National Identification Number (NIN) scheme, as well as reports of data breaches and the unlawful use of such data for surveillance.[227]

---

[223] Nwankwo, *supra* note 219 at 52

[224] Mannion, *supra* note 37 at 706

[225] Nwankwo, *supra* note 219 at 52

[226] Kunle Sanni, "Investigation - how Digital Loan Providers Breach Data Privacy, Violate Rights of Nigerians" (December 10, 2021) Online: Premiumtimes.ng. https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html [Permalink: https://go.exlibris.link/LLkD5VDH]

[227] Kelechukwu Iruoma, "Privacy Concerns Hobble Nigeria's Digital ID Push" (August 2 2021), Online: AllAfrica.com <https://go.exlibris.link/1qdz3x3v>

3.1.1 Development of a Regulatory Framework for Data Protection in Nigeria

Due to the lack of specific laws in Nigeria during the early stages of development of data protection regulations, the normative basis for developing a data protection framework was derived from the overarching right to privacy which is protected constitutionally but does not specifically reference data protection, with limited consideration of its cultural, economic and political dimensions.[228] Furthermore, judicial interpretation of data protection rights has largely been extrapolated from the constitutional right to privacy.[229] Due to the lack of a comprehensive framework, data protection regulations are inadvertently scattered across various legislations that aim to regulate how personal data is used in sectors such as banking and telecommunications, which rely heavily on personal data.

Several attempts to develop a comprehensive data protection framework have been made since 2005, Babalola, however, notes that these have been characterized by failed legislative attempts, judicial indifference, and political uncertainty.[230] One of the earliest attempts was the Data Protection Bill of 2011, which was reputed to be the first federal legislative proposal solely focused on data protection. This bill, however, failed to pass and was heavily criticized by scholars such as Makulilo, who asserted that it provided a low level of data protection in comparison to other African jurisdictions and was full of surprises.[231] Other notable attempts at creating a comprehensive legislation include the draft Data Protection Bill in 2015, the Personal Information and Data Protection Bill in 2016, and another draft Data Protection Bill in 2017.[232]

---

228 Abdulrauf & Fombad, *supra* note 217 at 117.

229 *Emerging Market Telecommunication Services v Barr Godfrey Nya Eneye* (2018) LPELR-46193.

230 Babalola, supra note 35 at 3.

231 Makulilo, *supra* note 12 at 25.

232 Babalola, *supra* note 35 at 3.

With the introduction of the Digital Rights and Freedom Bill in 2018, a new approach was taken, which led with a digital rights bill that incorporated data protection principles. Led by Civil Society Stakeholders such as the Paradigm Initiative, the bill was passed by the National Assembly in 2019, but it never became law because the President did not assent to the bill.[233] While the Digital Rights and Freedom bill was the closest attempt to enact data protection legislation, it suffered from the lack of distinction that is evident in Nigeria regarding the right to privacy and data protection in general. The Presidency emphasized this, stating that the main reason for declining assent was that the bill sought 'to cover too many technical subjects and fails to address any of them extensively.'[234]

The issuance of the Nigerian Data Protection Regulation (NDPR) in 2019, provided a temporary reprieve for stakeholders clamoring for data protection regulations. Despite being a subsidiary legislation, this was Nigeria's first comprehensive data protection framework. Further efforts have been made to develop a holistic framework with the Data Protection Bill 2020 introduced by the Federal Government through the Legal and Regulatory Reform Working Group (LWG) in support of the Federal Government's implementation of the Nigeria Digital Identification for Development (ID4D) Project.[235] In this regard, the World Bank, which is assisting the Federal Government in developing several components of a comprehensive National Identification Program, has identified the "development of a legal and regulatory framework that adequately protects individuals' personal data and privacy" as a major pillar and is currently providing support to develop a regulatory framework.[236]

---

[233] *Ibid* at 3.

[234] Solomon Fowowe, "Buhari Declines Assent to Digital Rights Bill, Four Others", (20 March 2019), online: AllAfrica.com <https://go.exlibris.link/0Gx1975y>.

[235] Bisola Scott, "A Review of the Nigerian Data Protection Bill 2020" (8 September 2020), online: Mondaq Business Briefing. link.gale.com/apps/doc/A634806812/ITBC?u=uvictoria&sid=summon&xid=8e7f1f2e. [permalink: https://go.exlibris.link/Zfs2JWgD].

[236] World Bank, "Nigeria Digital Identification for Development Project" (2020) online: worldbank.org https://projects.worldbank.org/en/projects-operations/project-detail/P167183.

The recent effort by the Nigerian government to develop comprehensive data protection laws demonstrate the increasing importance of data protection, with the central goal being to ensure that data processing in the country conforms to international standards, particularly the European Union's GDPR, and safeguards personal information. Indicating that these actions are considered necessary by the government for the growth of international trade and the IT sector. As identified a major impediment to this process has been the approach to creating such regulatory framework.

3.2 Analysis of The Nigerian Data Protection Framework

With the implementation of the GDPR, there is a general misconception that jurisdictions lacking data protection laws lack an adequate data protection framework, which has resulted in the enactment of GDPR-styled laws in countries such as Nigeria. Blume argues that this viewpoint is misleading because it ignores general and sectoral laws that aim to regulate the processing of personal data and, as an examination of provisions which restrict transfer of personal data to third countries reveals, the adequacy of a data protection framework is not solely dependent on the existence of an omnibus data protection law.[237] In this regard, a subsequent analysis of the Nigerian data protection framework will be constrained within the three broad evaluation criteria established by Article 45 (2) a-c of the GDPR.

3.3 Adequacy Assessment Criteria Under Article 45 (2) (a) GDPR

The provisions under the GDPR's first assessment criteria are extremely broad, and in some cases refer to principles with various meanings and applications. As a result, a detailed analysis of these criteria refers to the context within which these principles or concepts have been applied by the CJEU. This analysis adopts Wagner's approach of classifying the provisions of Article 45 (2)

[237] Blume, *supra* note 5 at 69.

(a) GDPR by breaking it down into general and specific requirements. The general criteria assesses the respect for the rule of law, fundamental rights and analyzes national security legislations in place, while the specific criteria focuses on available data protection legislations, including rules for the onward transfer of personal data to another third country, the implementation of such legislation, enforceable data subject rights, and effective administrative and judicial redress for data subjects.[238]

3.3.1 Adherence to The Rule of Law and Respect for Fundamental Rights and Freedoms

Nigeria has had a tumultuous history conforming to the principles of the rule of law, owing to the country's long period of military rule between 1966 and 1999. The usurpation of the existing political and constitutional order, accomplished primarily through constitutional suspension and attempts to oust the jurisdiction of the courts, was central to the authority of military administrations.[239] Attempts by the military to undermine the principles of the rule of law were, however, widely challenged by the judiciary, which consistently affirmed the primacy of the principle of separation of powers to the structure of the Nigerian system of government. In *Lakanmi v. AG Western State*, the Supreme Court fundamentally questioned the constitutional basis of the country's military decrees and edicts, holding that the military decree No. 45 of 1968 which summarily forfeited the assets of certain politically exposed persons amounted to legislative sentence and was ultra vires.[240] The Supreme Court also examined the legality of ouster clauses, which had the effect of stripping citizens of their constitutional right to seek redress in court, and determined that they were null and void.[241]

---

[238] Wagner, *supra* note 26 at 321.

[239] Mohammed Akanbi & Ajepe Shehu, "Rule of Law in Nigeria" (2012) 3:1 Journal of Law, Policy and Globalization 1-9 at 3.

[240] Lakanmi Vs. A-G. Western Region (1974) EGSLR 713 at 722.

[241] *Ibid.*

The transition to civilian rule in 1999 signified the beginning of a new era of governance, with the expectation that the rule of law would naturally thrive better in a democracy than in previous military regimes. In principle, the Nigerian government claims to be democratic, as it has held regular elections since 1999 and subscribes to several international instruments aimed at promoting respect for the rule of law and maintains an adherence to the application of known laws without intervention.[242] The *Constitution of the Federal Republic of Nigeria* serves as the foundational basis for the application of the rule of law in and provides for civil and political rights which are classified as "Fundamental Rights". Chapter IV of the constitution specifically recognize political and civil rights such as the right to life, personal liberty, and dignity, the right to a fair hearing, freedom of expression, privacy and family life, freedom of movement, freedom from discrimination, freedom of association, and freedom of religion.[243] Section 6 of the constitution vests judicial powers in the courts, which are empowered to decide questions concerning a person's civil rights and obligations.[244] The constitution also provides that a Court shall be formed in such a way as to ensure its independence and impartiality when exercising its powers.[245]

As the government is presumed to be founded on the principle of the rule of law, all official policies and actions are required to be carried out according to law. However, Okon, asserts that the rule of law is a farcical concept in Nigeria.[246] Criticisms of the constitution's drafting are central to this viewpoint, as scholars argue that dictatorial elements were retained due to the background and orientation of its drafters, who conferred enormous powers on the executive organ of

---

[242] *Constitution of the Federal Republic of Nigeria* (CFRN), LFN 1999 as amended c.23, s.135 (2). s.135 (2) provides that presidential elections must be held every four years. Since 1999 elections to various levels of government have been held consistently every four years, however, there have been concerns as to electoral violence and rigging.

[243] *Ibid* at s.33-42.

[244] *Ibid* at s.6(1).

[245] *Ibid* at s.6(6).

[246] Elijah Okon John, "The Rule of Law in Nigeria: Myth or Reality" (2011) 4:1 J Pol & L 211 at 212.

government.[247] The excessive powers conferred on the executive is a complete negation of the concept of separation of powers. This dictatorial influence was further entrenched by the continued presidential election of former military rulers, including General Olusegun Obasanjo from 1999 to 2007 and General Muhammad Buhari from 2015 till date. The arbitrary exercise of power by the executive, the docility of the judiciary, and the National Assembly's blind loyalty to the President and his party have significantly stifled the development of rule of law and weakened the capacity of the inbuilt mechanisms to check the executive's exercise of excessive powers.[248]

The obedience of court orders is a key indicator of compliance when evaluating adherence to the principles of the rule of law, but successive administrations have consistently disregarded judgment of Courts at various levels. In *Attorney-General of Lagos State v. Attorney-General of the Federation*, the Obasanjo led executive was reprimanded by the Supreme Court for withholding statutory funding to local governments in Lagos state without a court order for a purported constitutional breach.[249] The court determined that the proper course of action would have been to seek redress in a court of law rather than relying on self-help, which is not available to any government agency, and ordered that the allocation be released.[250] However the President failed to comply with the decision of the court and this decision was not complied with until a new administration took office.[251] The failure to comply with court orders continued with subsequent governments. Most recently, the presiding judge of the regional ECOWAS court, Justice Friday Nwoke, ruled that the Buhari-led government's willful disregard of five court orders to release on

---

247 *Ibid.*

248 Said Adejumobi, *Governance and Politics in Post/Military Nigeria: Changes and Challenges* (New York: Palgrave Macmillan, 2011) at 127.

249 *Attorney-General of Lagos State v. Attorney-General of the Federation* (2002) 1 WRN 1.

250 *Ibid*.

251 Proshare Nigeria, "Yar Adua orders release of Lagos N10.8b council funds", (24 July 2007), online: Proshare https://www.proshareng.com/news/Nigeria-Economy/Yar-Adua-orders-release-of-Lagos-N10.8b-council-funds/2659 [https://perma.cc/4RLA-J3YN]

bail Col. Sambo Dasuki, who was detained on corruption charges, was unlawful, arbitrary, and a mockery of democracy and the rule of law.[252]

Notwithstanding the provisions of the 1999 constitution, there has also been a consistent and widespread violation of fundamental rights and freedoms of citizens. As per the United States Bureau of Democracy, Human Rights, and Labor's 2020 Reports on Human Rights Practices, significant human rights violations in Nigeria included unlawful and arbitrary killings by both government and non-state actors, arbitrary detention by both government and non-state actors, political prisoners, arbitrary or unlawful interference with privacy, serious restrictions on free expression, the press, and the internet, including the existence of criminal libel laws.[253] The massacre of unarmed protesters who were protesting police brutality and arbitrary arrests on October 20th, 2020 orchestrated by officials of the Nigerian Army and Police is a clear case of state sanctioned killings which violate the fundamental rights of citizens.[254] Internet censorship measures, which culminated in the well-publicized restriction of access to popular microblogging network Twitter by the Federal Government in June 2021, is also indicative of a disregard for the right to free expression.[255]

The European Commission currently publishes a rule of law Report focused on member countries of the EU which identifies "key interdependent pillars for ensuring the rule of law" and while there has not been any official assessment of Nigeria's adherence to the rule of law principles, an analysis within the framework established may show that Nigeria falls substantially short of EU standard. This is supported by independent assessments by organizations such

---

[252] *Dasuki v Federal Republic of Nigeria* (2016) ECOWAS CJ, ECW/CCJ/JUD/23/16.

[253] U.S Department of State, 2020 Country Reports on Human Rights Practices: Nigeria (March 30 2021), Online: State.gov https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/nigeria/ [https://perma.cc/PF93-3C9D].

[254] Chidubem Iwuoha, and Ernest Aniche, "Protests and blood on the streets: repressive state, police brutality and #ENDSARS protest in Nigeria." (2021) 34:3 Security Journal 1-23 at 15.

[255] Wisdom Anyim, "Twitter Ban in Nigeria: Implications on Economy, Freedom of Speech and Information Sharing." (2021) 5975 Library Philosophy and Practice 1-14 at 3.

Freedom House, which currently rates Nigeria as partly free with a percentage of 45 percent in its annual study of political rights and civil freedoms around the world, compared to 98 percent for Canada.[256] The report emphasizes that while the electoral process and political engagement have improved significantly, there are still serious concerns about endemic corruption, extrajudicial executions by law enforcement, and the regular harassment and imprisonment of journalists covering politically sensitive themes.[257]

3.3.2 Relevant Legislation, Both General and Sectoral, Including Concerning Public Security, Defence, National Security and Criminal Law and The Access of Public Authorities to Personal Data

Given Nigeria's military and colonial history, state-sanctioned surveillance is pervasive.[258] Specified legitimate reasons for intelligence gathering and surveillance include national security, preventing or investigating crime, protecting and safeguarding economic well-being, and public emergency or safety interests.[259] However, it has been used by several Nigerian governments to gather intelligence, intimidate and harass opponents, critics, and leaders of civil society organizations.[260] Institutions responsible for national security and intelligence gathering, such as the Department of State Security (DSS), the Defence Intelligence Agency (DIA) and the National Intelligence Agency (NIA), were established by previous military regimes and have continued to function as state appendages under civilian rule.[261] In several cases, clandestine surveillance activities in violation of the law have been revealed, such as in 2013, when the Nigerian government secretly and in violation of contract procedures awarded a $40 million tender to the

---

256 Freedom House, "Nigeria: Freedom in The World 2021 Country Report" (2021), Online: freedomhouse.org <https://freedomhouse.org/country/nigeria/freedom-world/2021> [https://perma.cc/PE98-NDCT].
257 *Ibid.*
258 Ridwan Oloyede, "Surveillance Law in Africa: A Review of Six Countries Nigeria Country Report" (21 October 2021), Online: ids.ac.uk <https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Nigeria%20Country%20Report.pdf?sequence=7&isAllowed=y> [https://perma.cc/8H2J-TQ4P].
259 *Ibid* at 107.
260 *Ibid* at 104.
261 *Ibid.*

Israeli firm Elbit Systems for technology that would allow the state to intercept all internet activity and invade the privacy of users at will.[262] Also a Citizens Lab report in 2020, established that the Nigerian Defense Intelligence Agency purchased cyber-espionage tools, which it used to spy on the communications of opposition figures, journalists, and protesters.[263]

The most relevant pieces of legislation that authorises lawful data interception in Nigeria include the Terrorism Prevention Act (TPA), the Cybercrimes Act, and the Mutual Assistance in Criminal Matters Act (MACMA). Section 26 of the TPA, regulates intelligence gathering, and provides that the Attorney General, Inspector General of Police, or National Security Adviser may direct a communication service provider to retain communication data for the purpose of preventing a terrorist act or prosecuting offenders under the Act.[264] The Cybercrimes Act authorizes law enforcement officers to apply to a judge ex-parte for a warrant to intercept data in any computer system or computer network, as well as to use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format.[265] Section 38(1) of the act also requires service providers to keep traffic and content data for two years, while law enforcement agents are given the authority to request data from service providers.[266] More recently, the Mutual Assistance in Criminal Matters Act of 2019 allows for the exchange of surveillance information with other countries relating to the identification and location of criminal offenders; obtaining evidence; intercepting telecommunications; and converting electronic surveillance.[267]

---

[262] Emmanuel Ogala, "Exclusive: Jonathan Awards $40 Million Contract to Israeli Company to Monitor Computer, Internet Communication by Nigerians" (25 April 2013), Online: Premium Times https://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-toisraeli-company-to-monitor-computer-internet-communication-by-nigerians.html [https://perma.cc/TE3F-FJ9X].

[263] Bill Marczak et al, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles" (December 1, 2021), Online: The Citizen Lab <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/> [https://perma.cc/7SLM-AW3G].

[264] *Terrorism Prevention Act (TPA)*, 2013 as amended Gazette A27, at s.26.

[265] *Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015*, at s.45(2) (e) and (f).

[266] *Ibid* at s.38(1).

[267] *Mutual Assistance in Criminal Matters Act 2019*, at Part V.

The Nigerian Communication Commission (NCC) is the regulatory body in charge of internet service providers and telecommunications companies in Nigeria, and it has issued regulations and guidelines requiring service providers to intercept communications, decrypt encrypted communications, and provide communications data to law enforcement agencies.[268] The Nigerian Communications Regulations 2019 grants the NCC monitoring and enforcement powers and mandates that licensees shall keep records of call data under the Cybercrimes Act.[269] The NCC also introduced the Lawful Interception of Communications Regulations in 2019, which establishes a regulatory framework for lawful interception, collection, and disclosure of intercepted communications in Nigeria, and states that only authorized agencies, which are the Department of State Security, the Nigeria Police Force, and the Office of the National Security Advisor, may intercept communication data subject to obtaining a court order.[270] The regulation mandates service providers to install capabilities that permit interception and prohibits network providers from providing services that cannot be intercepted and monitored.[271]

The CJEU has established that, while lawful interception of personal data may be required to ensure national security, the principles of proportionality and necessity must be considered. International standards have also been established to ensure that appropriate safeguards, such as judicial authorization, effective independent oversight, transparency, and user notification, are in place to limit access to intercepted information. In this regard, the TPA 2013, as amended, introduced safeguards such as requiring interception of communication data to be subject to a warrant signed by a judge, and such order must specify the length of time the service provider must retain the communication data. The Cybercrimes Act also provides that a law enforcement

[268] *Nigerian Communications Commission Act*, LFN 2003, N.9 at s.4(i)
[269] *Nigerian Communications (Enforcement Process, etc.) Regulations* 2019, B 82 at reg. 8(1).
[270] *Lawful Interception of Communications Regulations* 2019 B105.
[271] *Ibid* at reg. 10-11.

officer may apply *ex-parte* to a Judge for a warrant to obtain electronic evidence in a criminal investigation; however, unlike the TPA, the Act does not specify how long such data can be retained and does not limit law enforcement access. The MACM Act also includes safeguards, ensuring that interceptions are limited to serious criminal situations.[272]

Despite the inclusion of some safeguards for lawful data interception, there are noticeable gaps that result in insufficient data protection provisions. While the TPA and Cybercrimes Act require a warrant before data can be intercepted, it does not specify a test of necessity or proportionality and instead gives the authorizing judge broad discretion to order surveillance measures.[273] There is no requirement under the identified laws for subject notification and an independent oversight mechanism.[274] The Cybercrimes Act also does not limit the type of law enforcement agencies that can intercept data and this has led to its abuse by different law enforcement agencies such as the Nigeria's Economic and Financial Crimes Commission (EFCC), which is notorious for conducting illegal searches in its fight against cybercrime.[275] The Cybercrimes Act's unrestricted access for law enforcement agencies to search any data contained in a computer network therefore raises concerns, especially where personal data of EU data subjects may be stored within the country.

3.3.3 Data Protection Legislation, Security Measures, Including Rules for The Onward Transfer of Personal Data to Another Third Country

Prior to 2019, there was no specific legislation governing data protection in Nigeria, which meant that the right to personal data protection was impliedly read in the Constitutional rights provision which protected citizens' privacy, their homes, correspondence, phone conversations,

---

272 MACMA, supra note 267 at s.55.

273 Oloyede, *supra* note 258 at 117

274 *Ibid.*

275 Kunle Sanni, "Despite Promising Rule of Law, Bawa's EFCC Sticks to Crude Tactics of Hotel, Home Invasions" (October 9 2021), Online: Premium Times <https://www.premiumtimesng.com/news/top-news/488886-despite-promising-rule-of-law-bawas-efcc-sticks-to-crude-tactics-of-hotel-home-invasions.html> [https://perma.cc/LMR7-PWWJ].

and telegraphic communications, as well as other sectoral laws with loose data protection provisions. The introduction of the Nigerian Data Protection Regulation (NDPR) in 2019 provided an omnibus regulatory framework that represented an evolution of data protection regulation and aimed to safeguard citizens' and people's rights to data protection in order to foster the integrity of commerce and industry in the volatile data economy.[276] It also aims to improve the secure exchange of data, the business operating environment, and the creation of sustainable jobs.[277] The NDPR was also supported by an Implementation Framework in 2020 which provides guidance and clarifies certain contentious provisions of the regulation.[278] NITDA stipulated that this framework should be read in conjunction but does not supersede the regulation.[279]

In this context, an analysis of data protection legislations in Nigeria will be undertaken, with a particular focus on the NDPR and the Implementation Framework, to determine whether the NDPR provides an adequate level of protection in comparison to the GDPR. The CJEU and the EC have established that adequacy is determined by applying an "essential equivalence" standard and must be satisfied that the legislation in question is sufficiently similar. As a result, this assessment will not include a side-by-side comparison of articles in both legislations but will instead focus on the core components of the GDPR, which include (i) Scope (ii) Definition of key terms (iii) Legal basis for processing (iv) Data Subject rights (v) Rules for the onward transfer of personal data to another third country (vi) Organizational Accountability (vii) Data protection by design. In analyzing each of these components, this section will determine if they are adequately addressed in the NDPR.

(i) Scope

[276] NDPR, *supra* note 13 at art.1.1.
[277] *Ibid.*
[278] *Nigerian Data Protection Regulation: Implementation Framework*, November 2020 at art. 2.
[279] *Ibid.*

The NDPR provides that the "regulation applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria".[280] This has the effect of exceeding the extraterritorial scope contemplated under the GDPR, as the GDPR applies to data controllers and processors who do not have a presence in the EU but conduct processing activities in the EU or offer goods or services to individuals located in the EU, it is specifically limited to data processing of personal data of data subjects who are in the EU.[281] Therefore a significant difference between the NDPR and the GDPR is that the NDPR governs the processing of personal data of Nigerian citizens located outside of Nigeria. However, implementing this provision is particularly complicated, and neither the NDPR nor the Implementation Framework specify how this extraterritorial scope will be implemented.

In terms of the organizations governed, the NDPR makes no distinction between private and public bodies, implying that it applies equally to government agencies and institutions, as well as private sector organizations that own, use, or deploy information systems. The Implementation Framework also states that NITDA shall deploy strategies and programs to improve electronic governance in public institutions, which indicates that it applies to government agencies.[282] While the NDPR did not identify any statutory and legal exceptions to the application of data protection provisions, the Implementation Framework emphasizes that the NDPR does not cover the use of personal data by government agencies in the pursuit of national security, public health, safety, and order, the investigation of criminal and tax offences, the collection and processing of anonymised data, and personal or household activities with no connection to a professional or commercial

[280] NDPR, *supra* note 13 at art.1.2.
[281] GDPR, *supra* note 8 at art.3.
[282] NDPR Implementation Framework, *supra* note 278 at art. 13.1.

activity.[283] The categories of processing that are excluded from the scope of application under the NDPR are similarly provided for under the GDPR.[284]

(ii) Definition of Key Terms

The definition of terms is critical to understanding how data protection legislation applies to both individuals and organizations. For example, whether an organization's information constitutes "personal data" will determine whether and to what extent such information is protected. The GDPR and the NDPR both provide similar definitions of "personal data", which is defined under the NDPR to mean:

> any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.[285]

Here, similar to the GDPR, the NDPR provides context by identifying that personal data can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers.[286]

---

[283] *Ibid* at art. 2.1.
[284] GDPR, *supra* note 8 at art. 2.2.
[285] NDPR, *supra* note 13 at art. 1.3 (xix).
[286] *Ibid*.

Both the GDPR and NDPR also provide similar definitions of "sensitive personal data", with the NDPR specifying that this means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, criminal records or any other sensitive personal information.[287] It is worth noting that, while the NDPR specifically categorises sexual orientation as sensitive data, this contradicts other established laws such as The *Same-Sex Marriage Act* signed into law in 2014 that effectively criminalizes lesbian, gay, bisexual, and transgender (LGBT) persons based on sexual orientation and gender identity.[288] Where exceptions to data protection provisions for criminal offences are applied, it means that sexual orientation is not specifically covered as sensitive data.

(iii) Legal Basis for Processing

The NDPR and the GDPR both provide that personal data can only be processed where there is a lawful basis for processing.[289] The NDPR states that processing is lawful only if one of the legal basis which include consent; when processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; compliance with a legal obligation to which the controller is subject; to protect the vital interests of the data subject or of another natural person; or performance of a task carried out in the public interest or in the exercise of official public mandate vested in the controller applies.[290] However, a significant omission here is that the NDPR does not recognise the data controller's legitimate interests as a legal ground for processing, whereas the GDPR specifies that this is a legal ground where it does not override the data subject's fundamental rights.

[287] *Ibid* at art. 1.3 (xxv).
[288] *Same Sex Marriage (Prohibition)* Act, 2013.
[289] NDPR, *supra* note 13 at art. 2.2.
[290] *Ibid*.

I argue that this omission has economic consequences for organizations because the legitimate interest ground is still one of the most flexible options for processing personal data.

The NDPR recognises consent as a legal basis to process personal data and imposes an obligation of disclosure and obtaining consent on the Data Controller. This requires that no data be obtained or processed unless the specific purpose of collection is disclosed to the data subject and consent is obtained prior to collection.[291] Such consent from a Data Subject must also have been obtained without fraud, coercion or undue influence.[292] The NDPR also provides that a Data Subject has a right to withdraw consent at any time, and must be informed of this right and the method to withdraw any prior given consent with ease.[293] Consent can be obtained through a statement, and when obtained in the context of a written declaration that also concerns other matters, it should be presented in a way that clearly distinguishes it from the other matters, in an intelligible and easily accessible form, and using clear and plain language.[294] In this regard, the NDPR and GDPR contain similar provisions regarding how consent must be obtained and withdrawn. The major distinction, in terms of the legal basis for processing, is that the NDPR contains no provisions that regulate consent by minors, whereas the GDPR states that where a child is under the age of 16, processing shall be lawful only if consent is given or authorized by the holder of parental responsibility over the child.

(iv) Data Subject Rights

The NDPR incorporates similar data subject rights established under the GDPR. The eight data subject rights established in Chapter III of the GDPR are a major component of the

[291] *Ibid* at art. 2.3 (1).
[292] *Ibid* at art. 2.3 (2).
[293] *Ibid* at art. 2.3 (2).
[294] *Ibid* at art. 2.3 (2) (b).

regulation.[295] Some of these rights, such as the right to be forgotten, are highly contentious, and their application in other jurisdictions has been heavily debated due to the practicality of establishing this right and the ambiguity of current rulings attempting to implement such a right in certain circumstances.[296] The NDPR however provides for most of these rights, including the right to be forgotten, where it affirms that a data subject has the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing.[297] The NDPR however unlike the GDPR does not provide detailed exceptions where these data subject rights may not apply and also does not specifically provide for the right to object to automated processing of personal data as established under Article 21 and 22 of the GDPR. The regulation however provides for the general right that a data subject must be informed of the existence of automated decision-making, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[298]

(v) Transfer To Third Countries

The NDPR anticipates situations in which data must be transferred to third-party countries or international organizations, and states that any such transfer of personal data is subject to the supervision of the Attorney General of the Federation (AGF), as well as providing that the supervising agency, NITDA may decide whether a foreign country or international organization in question provides an adequate level of protection.[299] The requirement for AGF supervision and an adequacy decision by NITDA is one of the clearest examples of GDPR provisions being

[295] GDPR, *supra* note 8 at art. 13-25.
[296] Franz Werro, *The Right to be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia* (Cham: Springer International Publishing, 2020) at 11.
[297] NDPR, *supra* note 13 at art. 3.1(h).
[298] *Ibid* at art. 3.1(l).
[299] *Ibid* at art. 2.11.

replicated in the NDPR without taking into account the practicality of implementing these provisions. This complication is evident from a combined reading of the provisions of GDPR Art 2.11 (a), which states that the NTIDA has the authority to determine adequacy, and Art 2.11 (b), which states that the AGF has the authority to determine adequacy while taking into account certain criteria listed. If implemented, the AGF's requirement for data transfer supervision creates bureaucratic bottlenecks for data controllers and processors transferring data outside Nigeria, by creating multiple regulatory layers and in determining what countries data can be transferred to. The Implementation Framework aims to resolve this complication but appears to worsen the situation by requiring specific information to be provided where data is being transferred abroad but does not specify to whom that information is provided.[300]

The NDPR also provides exceptions where data controllers and processors can transfer data to third countries in the absence of any decision by NITDA or AGF as to the adequacy of safeguards, which replicates the provision under Article 49 of the GDPR that provides for derogations for specific situations.[301] The Implementation Framework provides further exceptions where transfers are made by an organization seeking to transfer personal data to another entity within its group of companies or an affiliate company, and stipulates that such organization can utilize Binding Corporate Rules (BCR) or sign Standard Contracting Clauses.[302] This is also an importation of GDPR provisions, but the NDPR does not define what the Binding Corporate Rules entail or make provisions for the Standard contractual clauses that such organizations must adopt.

In summary, the NDPR provisions that govern international data transfers is one area where the replication of GDPR principles fails to achieve the desired effect and instead creates difficulties

[300] NDPR Implementation Framework, *supra* note 278 at art. 14.1.
[301] NDPR, *supra* note 13 at art. 2.12.
[302] NDPR Implementation Framework, *supra* note 278 at art 7.3.

for the regulatory agency, data controllers, and processors. While the Implementation Framework provides a whitelist of countries considered adequate, which includes a list of 40 countries, the list does not provide rigorous documentation indicating how such an adequacy decision was reached, which is a practice established by the EU. As a result, this list does not appear to meet the NDPR and GDPR's rigorous standards for determining adequacy.

(vi) Organizational Accountability

The NDPR integrates accountability as a principle which requires that organizations put in place appropriate technical and organizational privacy measures and be able to demonstrate the effectiveness of such measures when requested. These measures include mandating organizations that process personal data to display a simple and conspicuous privacy notice that data subjects can understand on all mediums in which they collect data.[303] The NDPR also states that organizations must develop security measures to protect personal data, which include, but are not limited to, protecting systems from hackers, installing firewalls, storing data securely with access restricted to specific authorized individuals, employing data encryption technologies, and developing organizational policy for handling personal data. [304] A written contract between a third party and Data Controller must also govern data processing by a third party.[305]

One of the novel provisions of the NDPR is the requirement that organizations who process personal data must appoint a Data Protection Officer (DPO), however such organizations may outsource data protection to a verifiably competent firm or person.[306] This exceeds the scope contemplated under EU regulations as while the GDPR mandates the appointment of a DPO, it

[303] NDPR, *supra* note 13 at art 2.5.
[304] *Ibid* at art 2.6.
[305] *Ibid* at art 2.7.
[306] *Ibid* at art 4.1 (2).

only applies to public bodies and organizations that process large amounts of personal data.[307] The NDPR also states that NITDA has the authority to register and license Data Protection Compliance Organizations (DPCOs), who on its behalf will monitor, audit, conduct training, and provide data protection compliance consulting to Data Controllers.[308] The functions of the DPCO however, are contradictory, as they have supervisory powers as well as the ability to consult for organizations, creating a clear conflict of interest.

Another provision that complicates implementation is the time-based requirement that all organizations conduct a thorough audit of their privacy and data protection practices. The NDPR provides a list of what is expected to be included in the audit and where an organization processes the personal data of more than a thousand data subjects within a period of six months, that organization is expected to forward a copy of the summary of the audit to NITDA.[309] Also, an organization that processes the personal data of more than two thousand data subjects in a period of 12 months must submit on or before the 15th of March of each year a summary of its data protection audit.[310] The Implementation Framework also requires Data Controllers and Processors to conduct a data protection audit within twelve months of incorporation and then on a yearly basis.[311]

The provisions for compulsory audits and appointment of a DPO hit at one of the major concerns of implementation with respect to data protection laws, as the Implementation of NDPR in Nigeria will have considerable impact on the technical competence of data controllers and

[307] GDPR, *supra* note 8 at art 37.
[308] NDPR, *supra* note 13 at art 4.1 (4).
[309] *Ibid* at art 4.1 (5) & (6).
[310] *Ibid* at art 4.1 (7).
[311] *Ibid* at art 3.2.

processors and may result in additional financial cost to small scale organizations.[312] This is a challenge that the Implementation Framework sought to address by restricting the provision for appointment of a DPO to organizations whose core activities involve the processing of the personal data of over ten thousand data subjects, processing sensitive personal data or obtaining critical national information.

(vii) Data Protection by Design

Data protection by design principles (DPbD), which is a concept in which privacy considerations are considered at all stages of an organization's business development, is not provided for explicitly in the NDPR in the same manner that the GDPR does. NTIDA however, incorporates this by introducing its underlying principles in its Implementation Framework such as by ensuring that a Data Protection Impact Assessment (DPIA) is completed for every new project undertaken by an organization and also that an effective breach response plan is in place. Art 3.2 of the Implementation Framework provides that in enhancing compliance and reducing liabilities, organizations must design and maintain systems to be data protection compliant and must show that their systems are built with data protection in mind.[313] This provides that if an organization intends to embark on a project that will involve the intensive use of personal data, a DPIA should be conducted to identify potential areas where breaches may occur and devise a method of mitigating such risks.[314] It also states that NITDA may request the submission of a DPIA from any organization if such processing activities are deemed to have a high impact on data subjects.[315]

---

[312] Mohammed Agbali et al, *Data Privacy and Protection: The Role of Regulation and Implications for Data Controllers in Developing Countries* (Cham: Springer International Publishing, 2020) at 214.
[313] NDPR Implementation Framework, *supra* note 278 at art 3.2(v).
[314] *Ibid* at art 3.2(viii).
[315] *Ibid*.

The NDPR did not include any provisions for data breaches; however, the Implementation Framework stepped in once more to introduce a data breach reporting and notification framework. According to this framework, organizations must self-report personal data breaches to NITDA within 72 hours of becoming aware of them, and this must be documented in the organization's data protection policy.[316] The Framework also specifies the content that must be included in the breach report and requires that a data subject be notified of a personal data breach that poses a high risk to the data subject's freedoms and rights.[317]

3.3.4 Effective Administrative and Judicial Redress for Data Subjects

The existence of data protection laws notwithstanding, European regulators contemplate that there must be an effective administrative or judicial mechanism for enforcing the rights of data subjects whose personal data may be transferred to a third country. The NDPR designates NITDA as the agency responsible for enforcing the regulation and provides that, in the case of civil remedies, NITDA has the authority to establish an Administrative Redress Panel (ARP), which is authorized by the regulation to investigate allegations of violation of the regulation, issue administrative orders pending the outcome of investigations, and determine appropriate redress for any violation of the provisions of the regulation.[318] The Implementation Framework also states that the ARP will be made up of accomplished information technology professionals, public administrators, and legal practitioners, and that its rules of procedure will be drafted by a panel of experts who will take into account fair hearing and transparency principles.[319] The NDPR and Implementation Framework also prioritize expedited resolution of cases by stipulating that cases must be resolved within 28 days.[320]

---

316 *Ibid* at art 3.2(ix).
317 *Ibid* at art 9.3.
318 NDPR, *supra* note 13 at art 4.2 (2), (3), (4).
319 NDPR Implementation Framework, *supra* note 278 at art 11.1.
320 NDPR, *supra* note 13 at art 4.2 (5).

Despite the implementation of several aspects of the regulation and the Implementation Framework, NITDA has failed to constitute the ARP, as Babalola notes that the Agency was silent on the creation of the ARP when listing its achievements in the 2020 NDPR Performance Report.[321] The NDPR, however, stipulates that data subjects have the right to seek redress in a court of competent jurisdiction, an avenue that public interest groups such as the Incorporated Trustees of Digital Lawyers Initiative have attempted to use to enforce data subject rights by filing a litany of cases in both State and Federal Courts. This has not been without challenges, such as in *ITDLI v. LT Solutions & Multimedia Limited*, where the state high court ruled that it lacked jurisdiction to rule on issues arising from federal legislation because there was no express provision in the legislation granting such powers to a state court.[322]

In *ITDLI v. Unity Bank Plc*, the Federal High Court held that provisions of the NDPR cannot be enforced through the fundamental right mechanism because it was not made pursuant to Chapter IV of the Constitution and Section 4.2 (6) of the NDPR makes it clear that a breach of the regulation will be considered a breach of the *NITDA Act*.[323] The court further held that the regulation is not a Constitution implementing instrument, and as such, it will be improper to enforce it through the Fundamental Right Enforcement Rules. Babalola contends that the Court's decision implies that the ARP is the appropriate mechanism for enforcing the provisions of the NDPR and establishes a condition precedent before approaching the courts.[324] In this regard, NITDA's delay in creating an administrative redress mechanism creates a gap in enforcement and determining what measures are available to Data Subjects to resolve data rights issues.

---

321 Babalola, *supra* note 35 at 7

322 *Incorporated Trustees of Digital Lawyers Initiative v. LT Solutions & Multimedia Limited* (Unreported) Suit No: HCT/262/2020

323 *Incorporated Trustees of Digital Lawyers Initiative (on behalf of data subjects whose personal data were exposed by the Unity Bank Plc) v. Unity Bank Plc* (Unreported) Suit No: FCH/AB/CS/85/2020.

324 Babalola, *supra* note 35 at 7.

3.4 Adequacy Assessment Criteria Under Article 45 (2) (b) GDPR

The second major pillar of the GDPR adequacy assessment criteria provides that an evaluation must consider the existence and effective functioning of one or more independent supervisory authorities with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, assisting and advising data subjects in exercising their rights, and cooperating with supervisory authorities from other states. According to the EC, such a supervisory authority must act completely independently in carrying out its tasks and exercising its powers, and it must also be free of any external influence, direct or indirect.[325] The GDPR also states that supervisory authorities must be appointed by a transparent body and be supported by legislation that outlines their duties and powers in detail. In this regard, The NDPR identifies the supervisory authorities responsible for ensuring compliance with the regulation as either NTIDA or any other statutory body or establishment having the government's mandate to deal solely or partly with matters relating to personal data.[326] As a result, an evaluation of the effectiveness of Nigeria's supervisory authority will center on NITDA's legal status as a regulator, its level of independence, and the duties and powers conferred by the NITDA Act and the NDPR.

The GDPR requires supervisory authorities to be appointed by a transparent body and to be supported by legislation that outlines their duties and powers in detail. Babalola, however, asserts that NITDA's functions in relation to data protection regulation are self-assigned and are not supported by its Act or any known regulatory framework.[327] NITDA was established in 2001 to oversee the implementation of the National Information Technology (IT) Policy and to coordinate the development and regulation of the Information Technology Sector.[328] In 2007, an

[325] GDPR, *supra* note 8 at art 51.
[326] NDPR, *supra* note 13 at art 1.3 (xxiv).
[327] Babalola, *supra* note 35 at 7.
[328] Ibid.

Act of the National Assembly expanded NITDA's mandate to include the creation of a framework for the coordination, monitoring, evaluation, and regulation of IT practices, as well as the development of guidelines for electronic governance and the monitoring of the use of electronic data interchange and other forms of electronic communication transactions.[329] This mandate serves as the foundation for NITDA's assumption of responsibility for data protection in Nigeria, however, Babalola further argues that the power to regulate IT practices, issue electronic governance guidelines and monitor electronic data interchanges should not be conflated with the authority to issue data protection regulations.[330]

Scott and Eke also note that the GDPR expressly makes provisions for the regulation of non-electronic data as well as electronic data; however, NITDA's powers as granted by the act are limited to the regulation of electronic data, implying that the NITDA does not govern data stored in non-computerized formats.[331] The NDPR complicates matters further by stating that the regulation applies to the processing of personal data regardless of the means by which the data processing is being or is intended to be conducted, implying that the NDPR intends to regulate non-computerised data.[332] In *Ondo State University v Folayan*, the Supreme Court held that a statutory body must act within the scope of the law that established it, and thus any attempt to regulate non-computerized data falls outside the purview of NITDA functions.[333] While there has not been any judicial process challenging the scope of NITDA's powers, this limitation is concerning because personal data collected in Nigeria is still mainly stored in paper-based forms, indicating that data subjects have limited protection.

---

329 NITDA Act, *supra* note 29 at s. 6 (a,c).

330 Babalola, *supra* note 35 at 8.

331 Bisola Scott & Sandra Eke, "NITDA's power to regulate non-electronic data" (July 10 2020), Online: Mondaq Business Briefing <https://www.mondaq.com/nigeria/privacy-protection/961436/nitda39s-power-to-regulate-non-electronic-data> [https://perma.cc/PFF4-Q9N2].

332 NDPR, *supra* note 13 at art 1.2 (a).

333 *Ondo State University v Folayan* (1994) 7 & 8 SCNJ (PT.1).

In terms of the level of independence envisaged by the EC, such a supervisory authority must act completely independently in carrying out its tasks and exercising its powers, and it must also be free of any direct or indirect external influence. NITDA, as it currently exists, is an Agency under the supervisory control of the Ministry of Communication and Digital Economy that reports to the Minister of Communications. The Agency's key actors include the Director-General and the Board; however, the appointment of the Chairman of the Board is subject to Ministerial recommendation and Presidential approval; and, while the President appoints the Director-General, he may be dismissed at any time on Ministerial recommendation.[334] The Act provides that the Minister may issue directives to the Director General or Agency relating generally to matters of policy, and it is the Agency's or Director General's duty to comply with them.[335] The Minister also has supervisory control over the financial accounts of the Agency since the Agency is required to submit a report every year that includes a copy of the audited accounts for that year.[336] Therefore it is established that the provisions of the *NITDA Act* make it clear that NITDA is not an independent supervisory authority in the manner that European Regulators envision, and is subject to the Minister's whims and caprices.

The EC also expects a supervisory authority to have broad powers to ensure the enforcement of personal data regulations. The NDPR, as a subsidiary legislation, derives most of its enforcement powers from the *NITDA Act* and the NDPR appears to broaden the scope of its powers by outlining a variety of enforcement measures, including mandatory audits and the power to issue fines. However, it has been argued that the NDPR exceeds the scope of enforcement powers conferred by the *NITDA Act*. For example, the NDPR states that a violation of any Data

334 NITDA Act, *supra* note 29 at s. 2(3).
335 *Ibid* at s.31.
336 *Ibid* at s.20.

Subject's privacy rights shall be liable, in addition to any other criminal liability, to a fine of 2% of the preceding year's Annual Gross Revenue or a sum of ten million Naira, whichever is greater.[337] NITDA exercised this power for the first time in August 2021, imposing a monetary sanction on Sokoloans, a digital lender found to have violated NDPR provisions and was unwilling to cooperate with the Agency.[338] Ayanbola et al. contends that this exceeded the penalty limits set by the *NITDA Act*, as the organization is only authorized to levy fines of up to five hundred thousand Naira. They also contend that the powers to impose sanctions as exercised under the NDPR are significantly limited, and in the Sokoloans case, ultra vires.[339]

It is surprising that there haven't been any significant attempts, both judicial or scholarly, to call NITDA's usurpation of the function of data protection regulation into question. It may appear that data protection scholars, digital rights activists, and legal practitioners are overjoyed to have what the World Bank described as a stopgap measure and have failed to thoroughly examine the suitability of NITDA's role as a supervisory authority.[340] However, as established by Greenleaf, it is clear that NITDA's regulatory power is built on shaky ground, and the imposition of more severe monetary penalties may expose the Agency to legal scrutiny.[341] The Agency lacks the independence expected of a supervisory authority because the Minister of Communications is heavily involved in the organization's activities. More importantly, due to its lack of independence, NITDA is unable to effectively regulate other government agencies, ministries, and departments

[337] NDPR, *supra* note 13 at art. 2.10.

[338] Tolulope Ayanbola et al, "Legality of the Imposition of a Fine on Soko Lending Company Limited by the National Information Technology Development Agency" (August 20, 2021), Online: Aluko-oyebode.com <https://www.aluko-oyebode.com/wp-content/uploads/2021/09/Legality-of-the-Imposition-of-a-Fine-on-Soko-Lending-Company-Limited-by-the-National-Information-Technology-Development-Agency_.pdf> [https://perma.cc/AU74-6ZYY].

[339] *Ibid.*

[340] World Bank, "Nigeria Digital Economy Diagnostic Report" (2019), Online: worldbank.org, https://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf [https://perma.cc/B49K-KZDA].

[341] Greenleaf, *supra* note 220 at 4.

that are more vulnerable to data breaches. This may also explain why the level of compliance by government agencies has been subpar.

3.5 Adequacy Assessment Criteria Under Article 45 (2) (c) GDPR

The third major criteria for assessing adequacy considers a country's international commitments or other obligations arising from legally binding conventions or instruments, as well as its participation in multilateral or regional systems, particularly in relation to the protection of personal data. As previously stated, the EC will view accession to Council of Europe Convention 108 favorably. While all Council of Europe members have ratified the treaty, African countries such as Cabo Verde, Mauritius, Morocco, Senegal, and Tunisia have also acceded to it despite being non-member states.[342] Notwithstanding Nigeria's relationship with the Council of Europe on other conventions such as the Budapest Convention on Cybercrime, the country has not been invited to join Convention 108.[343]

Nigeria has played an important role and actively participated in the negotiation and drafting of two data protection instruments. These are the ECOWAS Supplementary Act on Personal Data Protection, which was passed in 2010, and the African Union Convention on Cybersecurity and Personal Data Protection, which was passed in 2014. The Supplementary Act was designed to fill a legal void in the member states' national laws by providing a harmonized legal framework for data protection within the West African subregion.[344] It requires member states to enact legislation to regulate the collection, processing, transmission, storage, and use of personal data within each member state, as well as to facilitate the free movement of personal data

[342] Council of Europe, "Chart of Signatures and Ratifications of Treaty 108" (December 2, 2021), Online: coe.int <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty treaty num=108> [https://perma.cc/VN9Q-LZ29].
[343] T-CY Committee, "Nigeria Invited to Join the Budapest Convention on Cybercrime" (July 11, 2017), Online: coe.int <https://www.coe.int/en/web/cybercrime/-/nigeria-invited-to-join-the-budapest-convention-on-cybercrime> [https://perma.cc/SY87-RJH6].
[344] Supplementary Act on Personal Data Protection within ECOWAS, 16th February 2010, A/SA.1/01/10.

within the community.[345] The Supplementary Act is presumed to be part of the Nigerian data protection legal framework, but Babalola contends that the Nigerian Constitution, requires domestication of international treaties by publication in the official gazette before they become enforceable in Nigeria, and there is no evidence that the treaty has been domesticated.[346] The Supplementary Act, however, clearly creates legally binding obligations on member states by virtue of its annexation to the ECOWAS Treaty.[347]

In 2014, Nigeria also participated in the Adoption of the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention). The Malabo Convention addressed Africa's need for a harmonized regulatory and legal framework for data protection, and mandated African States to effectively set up legal frameworks strengthening fundamental rights, physical data protection, and privacy, while allowing the free flow of personal data across the continent.[348] The convention closely mirrors the provisions of the COE 108 convention; however, the Convention has yet to enter into force, which means it does not impose any legal obligations on AU member states. The Convention provides that the convention will only enter into force after 15 AU member states have ratified it, which has yet to happen as it has only been ratified by 8 member states.[349] While some obligations are created for states that have signed or ratified the convention before it enters into force, it should be noted that Nigeria has neither signed nor ratified the Convention, indicating that it has minimal effect.

While Nigeria has yet to ratify any of the relevant data protection conventions, regulators clearly recognise their importance, as the NDPR Implementation Framework, for example, states

---

345 *Ibid* at art 2.

346 Babalola, *supra* note 35 at 4.

347 Nwankwo, *supra* note 219 at 71.

348 Convention on Cyber Security and Personal Data Protection, African Union, June 27, 2014, at Preamble.

349 *Ibid* at art.36.

that all countries that are signatories to the Malabo Convention will be considered to have "adequate protection" within the meaning of the NDPR.[350] Certain regulatory practices, such as NITDA's continued function as a supervisory authority, however, are incompatible with the Malabo Convention's criteria, which require state parties to establish an independent administrative authority to oversee the processing of personal data.[351] It is clear that, while Nigeria respects the provisions of these international treaties, it has made only limited efforts to ratify them or incorporate their significant provisions into its regulatory framework.

3.6 Is Nigeria's Data Protection Framework Adequate?

Nigeria has made no significant efforts to obtain an EU adequacy assessment; however, it is clear from the provisions of the NDPR and Implementation Framework that a similar criterion for assessing the adequacy of other countries as provided under Article 45 (2) of the GDPR is also established under the NDPR. As Nigerian regulators use the same assessment criteria, it provides a reasonable basis for determining whether the Nigerian data protection Framework is adequate within the framework of the GDPR. A general assessment indicates that the Nigerian data protection framework, as it currently stands, is inadequate for a number of reasons.

Taking the first assessment criterion into account, I contend that, despite the existence of an electoral democracy in Nigeria, there are clear shortcomings in respect to the rule of law and fundamental human rights in the country. As highlighted in the analysis, major indicators of these are the disregard for court orders by successive administrations and Nigeria's performance on key rule of law indexes in comparison to countries in the EU. Excesses associated with access to the personal data of citizens by public and security officials are also influenced by a disregard for the rule of law and fundamental rights. While legislation relating to surveillance can be improved to

[350] NDPR Implementation Framework, *supra* note 278 at Annexure C (1).
[351] Malabo Convention, *supra* note 348 at art.11.

emphasize the importance of proportionality and necessity, a major concern is the disregard by public officials for the safeguards in these laws. In this regard any attempts by Nigeria to obtain an adequacy decision may necessitate a commitment by the government to advance key metrics which signify respect for the rule of law and fundamental rights.

With respect to the existence of data protection legislations the NDPR contains similar provisions to the GDPR in terms of assessing data protection laws and enforcement mechanisms, and because the standard contemplated does not expect a perfect mirroring of GDPR principles, the NDPR ideally meets the standard of "essential equivalence". The regulation has numerous significant limitations, such as the fact that it is a subsidiary legislation issued by a government agency rather than the national assembly, which calls its legitimacy into question. The NDPR is also plagued by implementation issues, as the lack of an ARP leaves data subjects with no clear path to seek redress. In this regard, I argue that the redress mechanisms as presently provided by the NDPR are ineffective. In terms of the existence of a supervisory authority, NITDA as it is currently constituted does not meet the EU's standard of independence and lacks the necessary powers to function effectively. Nigeria has also failed to ratify or domesticate the various regional data protection regulations to which it is a party, indicating a lack of commitment to participating in international data protection frameworks.

Overall, an assessment of Nigeria's data protection framework may not provide a clear picture of what standards are considered adequate by the EU; thus, the following chapter analyses the Canadian data protection framework, which has been adjudged adequate, to determine where gaps exist, and useful lessons can be drawn.

CHAPTER 4: AN ASSESSMENT OF THE CANADIAN DATA PROTECTION FRAMEWORK AND SIGNIFICANT LESSONS FOR NIGERIA

4.0 Introduction

Given the previous chapter's examination of Nigeria's data protection framework and the conclusion that obtaining an adequacy decision under the criteria established in that chapter may be difficult, it is useful to examine a jurisdiction with a framework similar to Nigeria's that has received a positive adequacy

assessment. In this chapter, I aim to highlight major factors that contributed to the EC's assessment of the Canadian data protection framework as adequate, and to identify lessons for developing the Nigerian data protection framework. This is accomplished by first tracing the evolution of Canada's data protection framework and highlighting key features in its development. Using the GDPR Article 45(2) assessment criteria, I then assess the Canadian data protection framework and compare it to Nigeria's framework. In concluding this chapter, I determine whether the Canadian framework is currently adequate and establish that there is room for improvement to meet the high standards of the GDPR while still providing salient lessons for Nigeria.

4.1 The Evolution of the Canadian Data Protection Framework

The Canadian data protection framework has been determined to be "adequate" by the European commission. This was not always the case, as the decentralized structure of the Canadian political system ensured that the development of data protection laws was a complicated process and achieved incrementally. In terms of the conceptual basis for data protection in Canada, Levin and Nicholson argue that Canada represents a middle ground between the notion of privacy as dignity, which allows for government intervention and regulation as required by the EU directive, and the notion of privacy as liberty, which is a feature of the North American data protection

framework's self-regulatory model.[352] While the early approach to data protection was based on self-regulation, Canada has in the last decade gravitated toward a comprehensive and consistent framework. In this regard, Canada's approach is unique in that it seeks to strike a balance between the EU's stringent data protection policies and the United States' laissez-faire approach, which are seen to be at opposite ends of a spectrum.

Bayley and Bennett establish that data protection laws for the public and private sectors, at the national and provincial levels, have evolved pragmatically in response to a variety of local, national, and international pressures.[353] With respect to the legal underpinnings of data protection, Section 7 of the Canadian Charter of Rights and Freedoms serves as a source of constitutional protection of the right to privacy.[354] While this section does not explicitly mention privacy, there is an emerging body of case law that supports the view that the reference to "liberty" can be inferred to encompass privacy.[355] Furthermore, Canada was one of the first countries to pass laws governing data collection and access to information in the public sector. However, for a variety of historical, political, cultural, and economic reasons, data protection in the private sector remained unregulated until the passage of the Personal Information Protection and Electronic Documents Act (PIPEDA) in 1999.[356] Bennett and Raab assert that Canada's initial approach to data protection was based on the assumption that privacy threats from the government are more serious than those

---

352 Avner Levin & Mary Jo Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground" (2005) 2:2 U Ottawa L & Tech J 357 at 391.

353 Robin Bayley and Colin Bennett, *Privacy Impact Assessments in Canada in David Wright and Paul de Hert, Privacy Impact Assessment* (New York; Springer 2012) at 162.

354 Canadian Charter of Rights and Freedoms, s 7, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

355 In *R. v. Jones*, [2017] 2 S.C.R. 696, the Supreme Court of Canada held that Personal privacy is essential to individual dignity, autonomy, and personal growth, and protecting personal privacy is essential to a free and healthy democracy.

356 Colin Bennett & Charles Raab, "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response" (1997) 13:3 The Information Society 245-263 at 255.

from the private sector.[357] This viewpoint has evolved in the decade since PIPEDA's implementation, with ongoing efforts to strengthen data protection in the private sector.

The current *Privacy Act,* which governs the public sector, was enacted in 1982 and addresses a person's right to access and correct personal information held by the Government of Canada. The Act also governs the collection, use, and disclosure of personal information by the government while providing services. The passage of a separate Act governing access to information and data protection stems from the belief that personal information protection should be a corollary to freedom of information, and that the various exemptions in both pieces of legislation should be consistent.[358] The practice of incorporating data protection and access to information in a single statute was later adopted by all provinces and territories.[359] The various Federal and Provincial Privacy Acts also established the Office of the Privacy Commissioner to oversee the Act's implementation and whose primary duty is to receive and investigate complaints, though they differ in the extent to which their decisions are binding and how they are enforced.[360]

Data protection regulations in the private sector emerged much later. Prior to this, there were a few privacy provisions scattered throughout the financial, consumer credit, and telecommunications industries.[361] Bennett maintained that the early framework for data protection in Canada was a patchwork of inconsistent and incoherent policies which created acute economic implications for Canadian businesses. A significant turning point in the development of an adequate data protection framework for the private sector was the Canadian government declaring

---

[357] *Ibid*.
[358] Bayley & Bennett, *supra* note 353 at 162.
[359] *Ibid.*
[360] *Privacy Act* R.S.C., 1985, c. P-21 at s.53.
[361] Bennett & Raab, *supra* note 356 at 259.

a formal adherence to the 1980 OECD Guidelines in 1984.[362] This prompted the creation of voluntary self-regulation rules, the most extensive of which was the Canadian Standards Association's negotiation of a certifiable standard for personal data protection.[363] This code was created to bring some consistency to data protection policy and practice in the private sector in Canada, and it involved adapting and revising the 1981 OECD Guideline to meet the Canadian environment, with reference to the EU Directive.[364]

Despite the creation of the CSA Model Code, there were concerns that the self-regulatory model did not adhere to the existing European requirements set under the then EU Data Protection Directive. The passing of PIPEDA was the next crucial step in protecting Canadians' personal privacy. The government of Canada had two goals in mind when it passed PIPEDA.[365] To begin with, it was seen as an important part of Canada's Electronic Commerce Strategy in terms of establishing trust and confidence.[366] The second major motivation for this legislation was to maintain crucial trade ties with the EU by complying with article 25 of the EU Privacy Directive, which allowed for data transfers with an adequate level of protection.[367] PIPEDA is based on earlier sectoral and self-regulatory efforts to protect personal information in the private sector and the principles of the CSA's Model Code were ultimately incorporated with modifications into the Act.[368] The Act also specifically applies to all private organizations in Canada unless a province has private sector data protection laws that have been determined to be substantially similar.[369] Till

---

362 Colin Bennett, "Adequate Data Protection by the Year 2000: The Prospects for Privacy in Canada", (1997) 11.1 International Review of Law, Computers & Technology 79-92 at 80.

363 *National Standard of Canada Entitled Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96.

364 Bennett, *supra* note 362 at 80.

365 Levin & Nicholson, supra note 352 at 379.

366 *Ibid*.

367 *Ibid*.

368 *Personal Information Protection and Electronic Documents Act*, SC 2000, c.5.

369 *Ibid* at s.4. Some provinces have private-sector privacy laws that are substantially similar to PIPEDA. Organizations that are subject to a provincial privacy law that is substantially similar to PIPEDA are generally exempt from it when it comes to the collection, use, or disclosure of personal information that occurs within that province. A provincial privacy law is considered substantially similar to PIPEDA if it provides equal

date, only Quebec, British Columbia, and Alberta, as well as Ontario's Personal Health Information Protection Act, have been adjudged to be substantially similar to PIPEDA.

From the foregoing, the lessons learned from other countries' legislative efforts to protect personal data were instrumental in shaping the current Canadian data protection framework. These lessons cover international data protection principles, exceptions to those principles, and how those principles have been applied to fit the Canadian context. The passage of PIPEDA was critical in Canada receiving a positive adequacy decision from the European Commission under the old Data Protection Directive. Despite the introduction of comprehensive provisions under the GDPR in 2016, Canada is still regarded as having an adequate data protection framework. Understanding the Canadian approach to data protection is critical in this context for identifying existing gaps in the Nigerian Framework and lessons that can be learned.

4.2 Assessing the Adequacy of the Canadian Data Protection Framework

The European Commission (EC) issued the Adequacy Decision 2002/2/EC in December 2001, in accordance with Article 25(6) of Directive 95/46/EC, confirming that Canada provides an adequate level of personal data protection.[370] It is important to note, however, that Canada's adequacy determination was limit to organizations that were under the jurisdiction of PIPEDA, which includes organizations that: fall under federal jurisdiction, such as banks, airlines, and telecommunications: works declared to be federal works or undertakings: and commercial activities involving the collection, use, or disclosure of personal information, whether under federal or provincial law.[371] PIPEDA also applies where a province has not passed substantially similar legislation, and if a province meets the substantial similarity test, the provincial privacy

privacy protection, contains the 10 PIPEDA fair information principles, provides for independent oversight and redress with the power to investigate, allows the collection, use and disclosure of personal information only for appropriate or legitimate purposes.

[370] *Commission Decision (EC) 2002/2, supra* note 17.

[371] *Ibid*

law applies, providing a benchmark of privacy regulations across Canada.[372] This division of authority is significant because the laws of provinces recognized as substantially similar to PIPEDA are not covered by the adequacy decision. The adequacy decision of the EC also expressly states that the "substantial similarity" exclusion applies only to processing activities within the province in question as PIPEDA applies if the processing involves another province or country.[373]

Article 2 of Implementing Decision (EU) 2016/2295, which amended Decision 2002/2/EC, states that the EC is required to monitor developments in the Canadian legal framework, including developments concerning access to personal data by public authorities, on an ongoing basis in order to assess whether Canada continues to provide an adequate level of personal data protection, and the adequacy decision was reaffirmed in 2006.[374] The GDPR, which replaced the Directive 95/46, specifies that existing adequacy decisions must be reviewed every four years.[375] In this context, while PIPEDA was assessed under Directive 95/46, a new assessment will be made in light of higher standards of protection set out in the GDPR.

For the purposes of this dissertation, an assessment of the adequacy of Canada's data protection framework will determine how Canada approaches data protection in accordance with the three broad criteria established in GDPR Article 45(2) (a-c), rather than the initial assessment standard established under Directive 95/46. This evaluation will also be limited to the Federal approach to data protection, with a specific focus on PIPEDA in comparison to GDPR provisions to determine whether they are "essentially equivalent." In identifying the various practices that the

---

[372] Industry Canada, "Process for the determination of Substantially Similar Provincial Legislation by the Governor in Council," Canada Gazette Part I, August 3 202. 2385-2389.

[373] Commission Decision 2002/2/EC, supra note 17.

[374] Innovation, Science and Economic Development Canada, "Sixth Update Report on Developments in Data Protection Law in Canada" (2019), Online: Ic.gc.ca https://www.ic.gc.ca/eic/site/113.nsf/vwapj/SixthUpdateReportonDevelopmentsinDataProtectionLawinCanada_en.pdf/$file/SixthUpdateReportonDevelopmentsinDataProtectionLawinCanada_en.pdf [https://perma.cc/LWP7-RY8R].

[375] GDPR, *supra* note 8 at Article 45(3).

EC considered to be evidence of PIPEDA's adequacy, shortcomings or similarities with the Nigerian data protection framework will be outlined.

4.3 Adequacy Assessment Criteria Under Article 45 (2) (a) GDPR

In tandem with the assessment of the Nigerian data protection framework, this criteria is divided into key sections which include: adherence to the rule of law and respect for fundamental rights and freedoms; relevant Public Security, Defence, National Security and Criminal Legislation, including concerns with respect to the access of Public Authorities to personal data; data protection legislation and security measures, including rules for the onward transfer of personal data to a third country; effective administrative and Judicial redress for data subjects.

4.3.1 Adherence to The Rule of Law and Respect for Fundamental Rights and Freedoms

As previously established, respect for fundamental rights and adherence to the rule of law are considerably difficult to define and assess and this is also the same with the Canadian legal framework. Currie asserts that the Canadian literature on the rule of law distinguishes between a "thin" or minimalist conception of the rule of law, which focuses on formal procedural rules, and a "thick" conception, which focuses on substantive aspects such as the absence of corruption and the exercise of fundamental rights in practice.[376] In this regard, there is a significant appreciation of other extrinsic elements in applying the principles of the rule of law in Canada which include access to justice, open and accountable government, accessible and impartial dispute resolution and just laws.

The principle of the rule of law and respect for fundamental rights have been fundamentally entrenched and, in some ways, intertwined in Canada. Watson asserts that Canada was fortunate to inherit the principles of the rule of law at its inception, and that these principles have

[376] Ab Currie, "In Canada the Rule of Law Is Mostly Thick" (1 April 2020), Online: CFCJ-FCJC.org <https://cfcj-fcjc.org/a2jblog/in-canada-the-rule-of-law-is-mostly-thick/> [https://perma.cc/QU2E-AR2S].

strengthened as Canada has evolved.[377] The adoption of the Canadian Charter of Rights and Freedoms in 1982, states in the preamble that "Canada is founded on principles that recognise the supremacy of God and the rule of law".[378] This was considered a significant milestone in the development of the rule of law and the entrenchment of fundamental rights as it was the first time the rule of law was specifically mentioned in a Canadian Constitutional enactment.

Similarly, to Nigeria, Canadian courts have been very active in maintaining and enforcing the rule of law as an important constitutional doctrine, and this has produced juridical effects in various contexts. In *Roncarelli v. Duplessis,* the Supreme Court of Canada considered the actions of Premier Duplessis of Quebec with respect to the cancellation of the liquor license of a Quebec restaurateur, because of his support for members of a religious denomination, and not for any reasons related to the legislation governing the liquor license.[379] The Supreme Court held that the Premier violated the Rule of Law because this action constituted an abuse of the Premier's powerful position and that he had acted arbitrarily and without good faith.[380] In *Reference re Secession of Quebec,* the Supreme Court emphasized that the rule of law was one of the fundamental tenets of the Canadian constitution, and that while the written constitution is supreme, unwritten constitutional principles also create substantive obligations.[381]

Bloodworth et al. however maintain that the Supreme Court has adopted a formal or "thin" definition of the rule of law focusing on the procedural aspects of the principle.[382] This was evident in the *Re Manitoba Language Rights,* where the Supreme Court faced a difficult situation involving

---

377 Jack Watson, "you don't know what you've got 'til it's gone: the rule of law in Canada" (2015) 52:4 Alberta L Rev 689 at 690.

378 *Charter of Rights and Freedoms,* supra note 354 at preamble.

379 *Roncarelli v. Duplessis*, [1959] S.C.R. 121.

380 *Ibid*.

381 *Reference re Secession of Quebec*, [1998] 2 S.C.R. 217.

382 Michelle Bloodworth et al, "The Rule of Law in Canada: A Global Template?", (2013) 31:2 National Journal of Constitutional Law 111 at 111.

Section 23 of the Manitoba Act, 1870, which required Manitoba statutes to be enacted in both English and French.[383] Manitoba passed the Official Language Act in 1890, which stated that all Manitoba statutes must be written in English. This Act was, in effect, an attempt to repeal a constitutional requirement.[384] As many Unilingual laws had been passed after the enactment of the Official Language Act, the Supreme Court ruled that nearly all of Manitoba's laws were unconstitutional. However, the invalid laws were deemed temporarily valid for the minimum period required for their translation, reenactment, printing, and publication. In reaching this conclusion, the Court relied on the rule of law as a constitutional principle, affirming that it has two components, the first of which is the supremacy of the law over government and individuals, and the second of which is the rule of law as a tool for securing social order.[385] In this context, the Court reasoned that a body of law must exist in order to set expectations for citizens and promote "normative order," and thus balanced the need to enforce the legislature's duty to comply with the Constitution while also ensuring the continued rule of law in order to avoid a legal vacuum.[386]

Concerning the “thick” conception of the rule of law, Currie asserts that one can conclude that the rule of law in Canada is "thick," but not uniformly so.[387] Currie's analysis is based on the World Justice Project's Rule of Law Index which in its most recent publication ranked Canada 12th out of 139 countries. Canada performed relatively well when compared to countries in the EU, ranking higher than Spain and France and has consistently improved on the ranking hovering between 11th and 17th position globally.[388] With a score of 0.90, Canada's best performance is in

---

383 *Re Manitoba Language Rights*, [1985] 1 SCR 721.

384 *Ibid*.

385 *Ibid*.

386 *Ibid*.

387 Currie, *supra* note 376.

388 World Justice Project, “WJP Rule of Law Index- Canada” (2021), Online: Worldjusticeproject.org, <https://worldjusticeproject.org/rule-of-law-index/country/Canada> [https://perma.cc/Y2F7-44DC].

the index's order and security component.[389] Other components of the rule of law index have high scores as well, including constraints on government powers (0.82), absence of corruption (0.82), fundamental rights (0.82), open government (0.80), and regulatory enforcement (0.80).[390] Canada's worst performance is in the civil justice component, where it ranks 22nd with a score of 0.70, leading Currie to conclude that "the rule of law in Canada is not uniformly thick. It is slightly curvilinear, with a thin spot on civil justice".[391]

When compared to Nigeria's performance on the same index, Canada's performance is put into better context. Nigeria is ranked 124th out of 139 countries evaluated with an overall score of 0.40, and it also performed poorly regionally, ranking 26th out of 33 Sub-Saharan African countries evaluated.[392] Nigeria scores poorly on the identified rule of law indices, such as the absence of corruption (0.32), order and security (0.34), criminal justice (0.40), fundamental rights (0.43), open government (0.42), and regulatory enforcement (0.44). (0.43).[393] Nigeria's best performance is in constraints on government power and civil justice, both of which are still relatively low at 0.50 and 0.48, respectively.[394]

Despite Canada's relatively high ranking on the Index, it is clear that deeper rule of law issues are being confronted, particularly in relation to its colonial legal history. Borrows recognises this in his analysis of the relationship between the Canadian legal system and Indigenous legal traditions, which he indicates has been marked by centuries of oppression of Indigenous rights and traditions.[395] Orkin further asserts this is most visible in the government's defiance to the

---

389 *Ibid.*

390 *Ibid.*

391 Currie, supra note 376.

392 World Justice Project, "WJP Rule of Law Index- Nigeria" (2021), Online: Worldjusticeproject.org, <https://worldjusticeproject.org/rule-of-law-index/country/Nigeria> [https://perma.cc/Y2F7-44DC].

393 *Ibid.*

394 *Ibid.*

395 John Borrows, *Canada's Indigenous Constitution* (Toronto, University of Toronto Press, 2010) at 169.

application of the rule of law in current federal policies and practices toward Canada's First Nations peoples, whom are being internally colonized in the country through "a long, deliberate, and ongoing process of cultural suppression, dispossession, breach of promise and trust, legislative and other oppression, as well as state and public discrimination and violence".[396] There are also other existing reports of rule of law infractions by the executive, such as violations of Conflict of Interest Act provisions by the Liberal Government led by Justin Trudeau.[397] These include notable reports such as the 2017 investigation into Trudeau's relationship with the Aga Khan Foundation, which discovered multiple violations of the legislation,[398] and the 2019 investigation into the SNC-Lavalin affair, which revealed publicly violations of the legislation.[399]

Despite these significant concerns, I argue that it is evident that the rule of law plays a critical role in Canada's social structure and has attained a significant constitutional status. Perhaps a clear indication of this is the ability of the Conflict of Interest and Ethics Commissioner to issue a report strongly criticizing the Prime Minister's role in the SNC-Lavalin Affair, which contrasts sharply with Nigerian institutions' limited capacity to provide independent governmental oversight.

4.3.2 Relevant Legislation, Both General and Sectoral, Including Concerning Public Security, Defence, National Security and Criminal Law.

Government agencies in Canada have conducted telecommunications surveillance since the invention of the telegraph, and each new mode of communication has been accompanied by new surveillance capabilities.[400] This access is not unrestricted as the Charter provides the

---

396 Andrew Orkin, "When the Law Breaks Down: Aboriginal Peoples in Canada and Governmental Defiance of the Rule of Law" (2003) 41:3 Osgoode Hall LJ 445-463 at 445.

397 *Conflict of Interest Act*, SC 2006, c 9, at s 2.

398 Canada, Office of the Conflict of Interest and Ethics Commissioner, The Trudeau Report, by Mary Dawson (Ottawa: CIEC, 20 December 2017).

399 Canada, Office of the Conflict of Interest and Ethics Commissioner, Trudeau II Report, by Mario Dion (Ottawa: CIEC, 14 August 2019).

400 Christopher Parsons and Adam Molnar, "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports" (2018) 16:1 CJLT 144 at 144.

constitutional basis for safeguards in Section 8 which establishes that everyone has the right to be secure against unreasonable search or seizure.[401] In *R v Spencer,* the Supreme Court recognized the concept of anonymity in deciding that an individual has a constitutionally protected privacy interest, by virtue of Section 8 of the charter and that the action of the police in obtaining this subscriber internet protocol information without prior judicial authorization amounted to an unreasonable search.[402] Koutrous and Demers also emphasize that various Canadian statutes and provisions (such as the Protection of Privacy Act, which, among other things, required federal and provincial governments to present annual reports detailing the number of electronic surveillance requests and approvals, how they were carried out, and their utility in securing convictions against alleged criminal offenders) have created an expectation of personal data privacy.[403]

In a response to terrorism post 9/11, Canada and its allies have enacted many laws and initiatives in the name of national security, some of which the Privacy Commissioner of Canada, Daniel Therrien argues went too far.[404]Through Public Safety Canada (PSC), which reports to the Minister of Public Safety, Canada appears to have a coordinated approach to data collection for national security purposes. The PSC unveiled Canada's first comprehensive counter-terrorism strategy in February 2012, with the goal of "countering domestic and international terrorism in order to protect Canada, Canadians, and Canadian interests."[405] This strategy identifies three primary federal government intelligence gathering organizations which include the Canadian Security Intelligence Service (CSIS), Communication Security Establishment Canada (CSEC),

---

401 *Canadian Charter of Rights and Freedoms,* supra note 354 at s.8.

402 *R v Spencer,* 2014 SCC 43.

403 Nicholas Koutrous and Julien Demers, "Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement", (2013) 11:1 CJLT 79 at 82.

404 Daniel Therrien, "From State Surveillance to Surveillance Capitalism: The Evolution of Privacy and The Case for Law Reform - Office of The Privacy Commissioner of Canada" (June 16, 2021), Online: Priv.gc.ca, <https://www.priv.gc.ca/en/opc-news/speeches/2021/sp-d_20210616/> [https://perma.cc/Z7VH-PKE9].

405 Public Safety Canada, "Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy" (2012), Online: Publicsafety.gc.ca <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx> [https://perma.cc/86EP-DK3J].

and the Royal Canadian Mounted Police (RCMP).[406] Other federal departments and agencies include the Department of National Defence (DND), the Department of Foreign Affairs and International Trade, the Canada Border Services Agency (CBSA), Transport Canada, and the Financial Transactions and Reports Analysis Center (FINTRAC).[407]

The CSIS and CSE oversee gathering information about national security. According to the Canadian Security Intelligence Service Act, the Service shall "collect, by investigation or otherwise, to the extent strictly necessary, and analyze and retain information and intelligence concerning activities that may on reasonable grounds be suspected of constituting threats to the security of Canada,"[408] The Act specifies that the Service may conduct investigations within or outside Canada. On the other hand, the Communications Security Establishment Act authorizes the CSEC to collect foreign signals intelligence.[409] The CSE Act however establishes that the activities of the CSEC must not be directed at Canadians or at any person in Canada and must not infringe the Canadian Charter of Rights and Freedoms.[410] CSEC collects foreign intelligence through its participation in a signal intelligence network run by Australia, Canada, New Zealand, the United Kingdom, and the United States, which is reportedly capable of intercepting phone calls and data traffic globally via various networks.[411] The CSIS Act also provides that if the CSE requests assistance, the CSIS has the authority to provide assistance on foreign intelligence gathering.[412]

---

406 *Ibid*.
407 *Ibid*.
408 *Canadian Security Intelligence Service Act* R.S.C., 1985, c. C-23 at s.12
409 *Communications Security Establishment Act* S.C. 2019, c. 13 at s.16
410 *Ibid* at s.22(1)
411 Christopher Parsons, "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance" (2015) 3:3 Media and communication 1-11 at 2.
412 CSIS Act, *supra* note 408 at s.16(1).

As stated in previous chapters, the EC contemplates the existence of personal data collection for National Security reasons but emphasizes the need for the entrenchment of the principle of "necessity" and "proportionality" in legislations and collection processes. The need to balance these concerns were evident in the criticisms of the *Anti-Terrorism Act* 2015.[413] Bill C-51, which became the *Anti-Terrorism Act* was an attempt to update the antiquated national security landscape, and a political and legal response to the terrorist attacks in 2014. Although Bill C-51 was positioned as a necessary set of legal amendments that would allow national security agencies to combat terrorism more effectively, Nesbitt argued that the Act created a series of authorities that were arguably unconstitutional such as the disruptive powers granted to the CSIS to limit any Charter right or Canadian law.[414] Furthermore, the Act contained provisions that created legal uncertainty, such as the broad information-sharing provisions under the *Security of Canada Information Sharing Act* (SCISA), which allowed government institutions to share information about activities but conflicted with the *Privacy Act's* information-sharing limitations.[415] The Privacy Commissioner of Canada was also assertive in his criticism of the Act, arguing that it failed to strike the proper balance by providing legislation that protects both Canadians' safety and privacy.[416]

It is important to note that debates over the *Anti-Terrorism Act* and the modernization of the national security landscape played a significant role in the 2015 Federal Election. With the election of the Liberal Party, which promised to repeal the "problematic elements of C-51", Public Safety Canada made concerted efforts to amend the Act to ensure that national security laws are

---

413 *Anti-terrorism Act*, 2015 S.C. 2015, c. 20.

414 Michael Nesbitt, "Reviewing Bill C-59, an Act Respecting National Security Matters 2017: What's New, what's Out, and what's Different from Bill C-51, A National Security Act 2015?" (2020) 13:12 School of Public Policy Publications 1-33 at 3.

415 *Ibid* at 5.

416 Daniel Therrien, "Op-Ed: Privacy Commissioner Raises Concerns About Bill C-51 - Office Of The Privacy Commissioner Of Canada" (March 6, 2015), Online: Priv.gc.ca https://www.priv.gc.ca/en/opc-news/news-and-announcements/2015/oped_150306/ [https://perma.cc/A2X5-DLSB].

consistent with the rights guaranteed by the Canadian Charter.[417] The 2017 *National Security Act* among other things amended but did not repeal the contentious provisions of the threat reduction measures of the CSIS under the *Anti-Terrorism Act*.[418] A major component of this reform was the introduction of safeguards with the enactment and establishment of the National Security and Intelligence Review Agency (NSIRA), whose mandate is to review any activity carried out by any national security or intelligence agencies in Canada.[419] The Act also created the role of Intelligence Commissioner, who is responsible for approving and overseeing ministerially authorized CSE activities related to electronic data collection, as well as CSIS activities related to the collection and retention of certain electronic data.[420]

When comparing Canada's collection of personal data for national security purposes to Nigeria's approach, I argue that recent changes to Canadian National Security Legislation aim to strike a balance between the need to expand personal data collection for national security purposes and constitutional and statutory safeguards against government intrusion in general. Nesbitt's arguments support this point of view, stating that the National Security Act is significantly broader in scope than previous legislations and addresses long-standing concerns about the lack of systematic review and oversight in the Canadian framework.[421] Unlike Nigeria's legislation and process for obtaining personal data for national security purposes, existing laws and practices aim to reflect the expectation of Canadians that their rights and freedoms will be safeguarded alongside their security. There is also a focus on establishing independent oversight bodies or mechanisms

---

[417] Public Safety Canada, "Parliamentary Passage of Bill C-59: The National Security Act, 2017 - Fulfilling Commitments to Address Former Bill C-51: Overview of New Measures" (2019), Online: Canada.ca <https://www.canada.ca/en/public-safety-canada/news/2019/06/parliamentary-passage-of-bill-c-59-the-national-security-act-2017---fulfilling-commitments-to-address-former-bill-c-51overview-of-new-measures.html> [https://perma.cc/HVK4-YLSL].

[418] *National Security Act*, 2017, SC 2019, c 13 at summary.

[419] *National Security and Intelligence Review Agency Act* S.C. 2019, c. 13, at s. 8.

[420] *National Security and Intelligence Committee of Parliamentarians Act*, S.C. 2017, Ch. 15.

[421] Nesbitt, *supra* note 414 at 26.

to ensure that the activities of national security agencies are reviewed, which is notably missing in the Nigerian framework.

4.3.3 Data Protection Legislation, Security Measures, Including Rules for The Onward Transfer of Personal Data to Another Third Country

As previously stated, Canada has federal and provincial privacy laws that govern private and public sector data collection. Even though PIPEDA is not an overarching data protection statute, the European Commission limited its adequacy decision to the Act but acknowledged the creation of substantially similar provincial laws that govern private sector processing for much of the business sectors in those provinces. As PIPEDA was enacted over 20 years ago, there are concerns that it may not be adequate in light of the GDPR, which was recently drafted and includes more robust provisions.[422] Within the established assessment framework, which focuses on (i) Scope (ii) Definition of key terms (iii) Legal basis for processing (iv) Data Subject rights (v) Rules for the onward transfer of personal data to another third country (vi) Organizational Accountability (vii) Data protection by design, a determination will be made as to whether or not PIPEDA provides adequate levels of protection in comparison to the GDPR and what lessons can be drawn from an Act which the EU considers to be adequate.

(i) Scope

PIPEDA was enacted with the overarching purpose of balancing two competing interests, which are the collection, use and disclosure of personal information in a manner that recognizes the right to privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[423] The act applies to all private sector

[422] Colin Bennett, "Is Canada Still 'adequate Under the New European General Data Protection Regulation?" (8 August 2016), Online: colinbennett.ca, <https://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-new-general-data-protection-regulation/> [https://perma.cc/7KQG-9ZGA].

[423] PIPEDA, *supra* note 368 at s.3.

organizations in respect of personal information that is collected, used or disclosed in the course of commercial activities and also to personal information that is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.[424]

The application of the PIPEDA only for commercial purposes is based on the constitutional limit on the federal government's powers in Canada. Because the federal government's ability to regulate privacy is limited, PIPEDA was carefully drafted to ensure it did not overstep constitutional bounds. Bennett, however, questions PIPEDA's comprehensiveness considering its constitutional limits as much of the non-profit sector and employee personal information, which is regulated by provinces, tends to fall between the cracks of the Canadian privacy regime.[425] PIPEDA also has a limited extraterritorial scope, which reflects an understanding of the country's constitutional limitations. This contrasts with the NDPR, which aims to regulate personal data collection of Nigerian data subjects outside jurisdiction. In this context, NDPR drafters should consider the implications of extraterritoriality to ensure that such provisions are implementable and within constitutional limits.

(ii) *Definition of Key Terms*

Under PIPEDA, the definition of key terms is considerably limited in comparison to the NDPR and GDPR. PIPEDA makes use of the term "personal information," which is defined as "information about a specific identifiable individual" but does not highlight what information will be personal information.[426] This creates considerable limitations as employee information is not considered to be personal information. The act also defines "commercial activity" as any

[424] *Ibid* at s.4(1).
[425] Bennett, supra note 422.
[426] PIPEDA, *supra* note 368 at s.2(1).

commercial transaction, act, or conduct, including the selling, bartering, or leasing of donor, membership, or other fundraising lists.[427] In this context, the definition of commercial activity, while limited, has been broadened by the Court in *Rodgers v. Calvert* to include Nonprofits that collect, use, or disclose personal information during commercial activity.[428] It is important to note that PIPEDA does not define certain key terms, such as sensitive information, or provide examples of what constitutes information about a specific individual and the NDPR and GDPR provide more details and are more comprehensive in this area.

(iii) Legal Basis for Processing

Consent is the primary legal basis for data processing under PIPEDA. The fundamental principles of consent as outlined state that consent is "required for the collection, use, or disclosure of personal information, except where inappropriate."[429] To meet the knowledge and consent criteria, organizations must "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used," and such consent must be meaningful by ensuring that "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed."[430] Furthermore, the Act states that consent is not permanent and can be revoked, and it also contains certain exceptions under which an organization may collect, use, or disclose personal information without an individual's knowledge or consent.[431]

Bennett identifies the legal basis for the processing of personal data as an area where PIPEDA needs to improve.[432] This is evident from the fact that, unlike the GDPR and NDPR,

---

427 *Ibid*.
428 *Rodgers v. Calvert*, 2004 CanLII 22082 (ON SC) at Para 56.
429 PIPEDA, *supra* note 368 at Schedule 1 (4.3.1).
430 *Ibid* at Schedule 1 (4.3.2).
431 *Ibid* at Schedule 1 (4.3.8).
432 Bennett, *supra* note 422.

PIPEDA does not include any other legal basis for processing other than consent and makes no specific provisions for minors' consent.

(iv) Data Subject Rights

In Canada, data subject rights are an essential component to the privacy-protection framework and these rights which are referred to as Fair information principles set the ground rules which govern the collection, use and disclosure of personal information and are included in the 1st schedule to the Act.[433] They form the basis of an individual's right to have control over his/her data. The Fair Information principles are derived from OECD Guidelines and mirror the rights included under the GDPR. Notably PIPEDA does not include new rights included in the GDPR including the contentious right to be forgotten, the right to portability nor does it include any provisions regarding automated decision making.[434]

(v) Rules For the Onward Transfer of Personal Data to Another Third Country

The processing of personal information by a third party located outside of Canada is not restricted by PIPEDA. The rationale for this is that PIPEDA is intended to support and promote electronic commerce, and the global interdependent economy is dependent on international information flows.[435] However In contrast to the GDPR's state-to-state approach, Canada has adopted an organization-to-organization approach that is not based on the concept of adequacy, as organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement under PIPEDA.[436] PIPEDA further provides that organizations must use contractual or other means to provide a comparable level of protection

[433] PIPEDA, supra note 368 at 1st schedule.

[434] Bennett, *supra* note 422.

[435] Office of the Privacy Commissioner, "Guidelines for Processing Personal Data Across Borders - Office of The Privacy Commissioner Of Canada" (2009), Online: Priv.gc.ca https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/ [https://perma.cc/Y629-4LJN].

[436] PIPEDA, *supra* note 368 at Schedule 1 (4.1.1).

while the information is being processed by a third party.[437] This is in stark contrast to the Nigerian approach, which adopted the EU's adequacy model. Implementing an adequacy standard may be relatively difficult and a time-consuming process for countries to implement and as such Nigeria should consider adopting the Canadian method of transferring the responsibility of ensuring secure data transfer to organizations.

(vi) Organizational Accountability

Canada applies the same basic tenet of privacy principles to organizations' handling of personal information established under the GDPR. The accountability principle establishes that an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing.[438] PIPEDA also provides that an organization must implement procedures to protect personal information, establish procedures to receive and respond to complaints or questions, train staff, and be transparent about all these procedures and practices.[439]

In terms of the appointment of a Data Protection Officer, PIPEDA states that an organization must name an individual or individuals who will be held accountable for the organization's adherence to the fair information principles.[440] In contrast to the GDPR and NDPR, I argue that Canada walks a fine line between recognizing the need for an individual to be responsible for data protection while also refraining from making such an appointment mandatory due to the financial implications for commercial entities. However, a clear definition of the role and qualifications of such a person is conspicuously absent.

[437] *Ibid* at Schedule 1 (4.1.3).
[438] *Ibid* at Schedule 1 (4.1.1).
[439] *Ibid* at Schedule 1 (4.1.4).
[440] *Ibid* at Schedule 1 (4.1.2).

(vii) Data Protection by Design

Currently, there is no provision in PIPEDA dealing with data protection by design, and the lack of such a provision has not gone unnoticed. Daniel Therrien, Canada's Privacy Commissioner, has identified data protection by design as a significant difference between PIPEDA and the GDPR.[441] Furthermore, the Standing Committee on Access to Information, Privacy, and Ethics clearly believes that a data protection by design framework like the GDPR is required, and some believe that privacy by design will be a contentious issue when the adequacy of PIPEDA is evaluated.[442]

In comparison to Nigeria, the NDPR, despite replicating the provisions of the GDPR, does not explicitly provide for Data Protection by Design principles, but does refer to them in its Implementation framework. I argue that the references in the Implementation Framework have no connection to the NDPR, making them unimplementable. Nigeria, like Canada, can benefit from incorporating clear data protection by design principles into its legislation to ensure compliance with GDPR standards.

4.2.3 Effective Administrative and Judicial Redress for Data Subjects

In Canada, primary responsibility for oversight of PIPEDA rests with the Office of the Privacy Commissioner and the Federal Court. This is referred to as an ombudsman model which provides redress for violations of personal data privacy rights. In *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, the court described the Privacy Commissioner of Canada as an "administrative investigator" with a range of powers, including the ability to initiate her own investigations and audits (with reasonable grounds) and the power to compel evidence and enter

[441] ETHI, Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act, February 2018.

[442] Standing Committee on Access to Information, Privacy and Ethics: Parliament. House of Commons, "Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act: Report of the Standing Committee on Access to Information, Privacy and Ethics" (Ottawa, Standing Committee on Access to Information, Privacy and Ethics, 2018).

premises when conducting investigations.[443] The OPC may also issue specific guidance as to the application of the Act. While the Commissioner has the authority to encourage compliance by naming respondent organizations when it is deemed in the public interest, he has no direct enforcement powers.[444] The Commissioner may only apply to the Federal Court in limited circumstances to have the Court hear certain issues raised in complaints.[445] The Court then has a range of enforcement powers which include the power to issue PIPEDA compliance orders, publish notices, issue corrections, or award damages to the complainant.[446]

The OPC's investigative powers are evident in several decisions, including the 2008 investigation of Facebook in response to a formal complaint about certain Facebook privacy policies and procedures. In 2009, the OPC issued a report criticizing Facebook's process of providing a sufficient knowledge basis for meaningful consent.[447] Even though the OPC did not find that Facebook had acted deceptively or misrepresented its activities, it was determined that the service provider had not met its PIPEDA knowledge and consent obligations.[448] The OPC then provided a list of recommendations, which were accepted and implemented by Facebook.[449] The courts have also sought to clarify some of PIPEDA's more contentious provisions, such as in *A.T. v. Globe24h.com,* where the federal court ruled that PIPEDA applied to organizations operating outside of Canadian borders who utilize personal data of Canadian data subjects.[450]

---

443 *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, [2008] 2 SCR 574 at para 20.

444 Colin Bennett, "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas" (2003) 46:2 Canadian Public Administration 218-242 at 226.

445 *Ibid*.

446 PIPEDA, *supra* note 368 at s.12(1).

447 Elizabeth Denham, 'Commissioner's Findings - PIPEDA Case Summary #2009-008: Report of Findings: CIPPIC V. Facebook Inc. - Office of The Privacy Commissioner of Canada' (19 July 2009), online: priv.gc.ca <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/> [https://perma.cc/A22N-5QGH].

448 *Ibid*.

449 *Ibid.*

450 *A.T. v. Globe24h.com* [2017] 4 FCR 310 at Para 53.

The OPC has expressed concern that the PIPEDA enforcement model is becoming increasingly out of date.[451] Because of its technology-neutral, principled-based approach, PIPEDA was regarded as a pioneer in data protection legislation when it was introduced in 2000. The introduction of stricter enforcement powers under the GDPR, on the other hand, raises the issue of ensuring that data protection authorities are given stronger powers commensurate with the increasing risks to personal information. This has resulted in a clamor from the OPC and recommendations that PIPEDA be reformed to provide for stronger enforcement powers, such as statutory damages administered by the Federal Court, granting the Commissioner the authority to make orders, or granting the Commissioner the authority to impose administrative monetary penalties.[452]

The Canadian approach to providing redress represents a distinct approach to ensuring that data subjects' rights are guaranteed and that effective mechanisms are in place to challenge compliance. As previously stated, while the NDPR provides for administrative monetary penalties, there is no proper enforcement structure in place, and the courts have a limited role in providing judicial oversight or interpretation. In this regard, future amendments to Nigerian data privacy legislation can take an approach that identifies appropriate mechanisms for seeking redress or providing guidance, as well as creating a proper framework for the judiciary to support enforcement and oversight.

4.4 Adequacy Assessment Criteria Under Article 45 (2) (b) GDPR; Independence of Supervisory Authority

Following the passage of the Privacy Act, which governs the personal information-handling practices of federal departments and agencies, the Office of the Privacy Commissioner

---

[451] Office of the Privacy Commissioner, "The Case for Reforming the Personal Information Protection and Electronic Documents Act - Office of The Privacy Commissioner of Canada" (May 2013), online: priv.gc.ca <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/> [https://perma.cc/27SH-B24C].

[452] *Ibid*.

of Canada (OPC) was established in 1983.[453] When the Personal Information Protection and Electronic Documents Act (PIPEDA) was fully implemented in 2004, the OPC's responsibilities were extended to the private sector.[454] The OPC is an Officer of Parliament who reports directly to Parliament on issues concerning Canadians' privacy rights. Officers of Parliament are regarded as independent actors who provide oversight over a specific area of concern.[455] While the officers' specific roles and mandates vary greatly depending on the subject matter, they share a number of key characteristics including: a method of appointment, a mandate and term in office defined by statute, a reporting obligation to one or both houses of Parliament, and independence from the government of the day.[456] They also share a common goal of improving government accountability by providing independent and expert information, analysis, and oversight to Parliament.[457]

The Privacy Act establishes the appointment of the Privacy Commissioner, Assistant Privacy Commissioner, and Office Staff. The Act provides that the Governor in Council appoints a Privacy Commissioner after consulting with the leader of each recognized party in the Senate and House of Commons and receiving Senate and House of Commons approval by resolution.[458] The Privacy Commissioner is appointed for a seven-year term, but may be removed for cause by the Governor in Council at any time on the advice of the Senate and House of Commons.[459] The Privacy Commissioner is also eligible for reappointment after the expiration of a first or subsequent term of office for a period of no more than seven years.[460] The Act also provides for remuneration, stating that the Privacy Commissioner shall be paid a salary equal to that of a judge

---

[453] *Privacy Act*, supra note 353 at s.53(1).

[454] PIPEDA, supra note 368 at s.12(1).

[455] Gwyneth Bergman & Emmett Macfarlane, "Protecting Privacy? Government and Parliamentary Responsiveness to the Privacy Commissioner of Canada" (2021) 64:3 Canadian Public Administration 437-456 at 439.

[456] *Ibid*.

[457] *Ibid.*

[458] *Privacy Act*, *supra* note 360 at s.53(1).

[459] *Ibid* at s.53(2).

[460] *Ibid* at s.53(3).

of the Federal Court other than the Chief Justice, as well as provision for expenses incurred in the course of performing official duties.[461] The Privacy Commissioner is also required on request by the minister of justice to present a report to Parliament within a certain time frame.[462] The Act also includes similar provisions for the appointment, remuneration, and removal of an unspecified number of Assistant Privacy Commissioners, whose terms are limited to five years subject to reappointment.[463]

As previously stated, despite performing a wide range of functions, the Privacy Commissioner has limited enforcement powers. In 2015, a small step forward was made with the passage of the *Digital Privacy Act*, which amended PIPEDA.[464] The Privacy Commissioner was given the authority under the new amendment to enter into compliance agreements with organizations to ensure that they comply with PIPEDA.[465] These compliance agreements are reached when the OPC has reasonable grounds to believe that an organization has committed, is about to commit, or is likely to commit an act or omission that may be in violation of PIPEDA.[466] An organization bound by a compliance agreement agrees to take certain steps to comply with PIPEDA, which prevents the OPC from filing or continuing a court application under PIPEDA in relation to any matter covered by the agreement.[467] Where an organization fails to live up to commitments in an agreement, the OPC may: (1) apply to the court for an order requiring the organization to comply with the terms of the agreement; or (2) initiate or reinstate court proceedings under PIPEDA.[468]

---

[461] *Ibid* at s.54(2).
[462] *Ibid* at s.60(2).
[463] *Ibid* at s.56 & 57.
[464] *Digital Privacy Act* (S.C. 2015, c. 32).
[465] *Ibid* at 17.1 (1).
[466] *Ibid.*
[467] *Ibid* at 17.1(3).
[468] *Ibid* at 17.2 (2).

Even though both countries have different government systems, the OPC's status as an independent supervisory authority teaches Nigeria a valuable lesson in developing its data protection framework, as the precise definition in the *Privacy Act* of the OPC's role, mode of appointment, and functions is distinguishable from the NITDA's complicated and contentious status as a regulator. The statutory provisions also serve as the foundation for the independence of the OPC. When attempting to identify the proper body responsible for data protection within a particular jurisdiction, a clear identification of the Supervisory Authority provides direction to data subjects who seek redress as well as to enforcement authorities in other jurisdictions.

4.5 Adequacy Assessment Criteria Under Article 45 (2) (c) GDPR

Canada actively participates in international fora such as the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) in initiatives aimed at improving and expanding the global interoperability of privacy frameworks.[469] With respect to the OECD, Canada participated in the Expert Group which produced the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[470] The Guidelines have been extremely influential in Canada, where it was adopted by the Canadian Standards Association's as the starting point for the development of the Model Code for the Protection of Personal Information.[471] This broke down the OECD's eight principles into ten data protection principles. The ten principles were subsequently incorporated as a schedule to Canada's PIPEDA. Canada also continues to contribute to the review of the OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of

[469] ISED Canada, *Supra*, note 374.
[470] *Ibid.*
[471] *Ibid*.

Personal Data as a member of the OECD Privacy Expert Group, established to provide advice on the review of its implementation.[472]

In terms of APEC, Canada is a signatory to the APEC Privacy Framework and its system of Cross-Border Privacy Rules (CBPR) framework, and it played a key role in its development in the early 2000s.[473] Bennett, however, argues that the APEC Framework's impact in Canada has waned as a critical aspect of the system's operation, which is the designation of "accountability agents" who provide oversight and receive consumer complaints has not been fulfilled.[474] Canada also participates in the Data Privacy Sub-Group, which is revising the Cross-Border Privacy Rules (CBPR) System to reflect the updated APEC Privacy Framework.[475] Furthermore, Canada is taking part in APEC/EU discussions aimed at updating the 2014 Referential on Personal Data Protection and Privacy Requirements of BCR and CBPR, as well as investigating the concept of certification as it relates to the GDPR and the CBPR.[476]

Notably, Canada has not acceded Convention 108, and Bennett contends that accession will benefit Canada, including the possibility of extending its adequacy status with the European Union under the GDPR.[477] Bennett further prioritizes Canada as one of the countries that may accede to Convention 108, citing the fact that it is one of only six countries that meet all of the criteria for accession and has already been declared adequate under EU rules.[478]

---

[472] *Ibid.*

[473] Colin Bennett, "The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession" (2020), online: Center for International Governance Innovation https://www.cigionline.org/publications/council-europes-modernized-convention-personal-data-protection-why-canada-should/ [https://perma.cc/FB9C-54NT].

[474] *Ibid* at 8.

[475] ISED Canada, *supra* note 374.

[476] *Ibid.*

[477] Bennett, *supra* note 473 at 8.

[478] *Ibid.*

Despite not acceding to Convention 108 Canada actively contributes to the development of international privacy standards, which it has adopted and also incorporated into PIPEDA. This contrasts with Nigeria's limited role in international privacy frameworks, as well as its lack of commitment to the conventions and instruments to which it is a party.

4.6 Is Canada's Data Protection Framework Currently Adequate?

In determining Adequacy, the EU Commission must be convinced that the Canadian data protection framework conforms to the standards set out in Article 45(2) of the GDPR. A major factor in this determination will be a determination as to whether PIPEDA is "essentially equivalent" to the GDPR. The former Directive 95/46 was used to conduct an initial assessment of PIPEDA's adequacy, and Bennett contends that PIPEDA may be outdated as it has not been updated to reflect a changing privacy landscape, particularly with the comprehensiveness of the GDPR. Although PIPEDA addresses core GDPR concepts in an "essentially equivalent" manner, the Act does not contain specific provisions that address contemporary issues which are included in the GDPR. As a result, the Consumer Privacy Protection Act (CPPA) and the Personal Information and Data Protection Tribunal Act (Bill C-11) were proposed to replace the PIPEDA. The bill is part of an ambitious plan to put in place a Digital Charter, which is a broad policy framework intended to guide Canada's overall digital policy.[479] Bill C-11 is also an attempt to modernize Canada's data privacy legislation, with the goal of ensuring that Canada retains its adequacy status, which is set to be reviewed in 2022.

Despite the limitations identified, there are some lessons from PIPEDA that can be used in drafting a comprehensive data protection legislation. The purpose and scope of PIPEDA clearly reflect a well-thought-out way of regulating commercial entities' access to personal data, while

[479] Government Canada, "Bill Summary: Digital Charter Implementation Act, 2020 - Innovation for A Better Canada" (11 November 2020), online: ic.gc.ca https://www.ic.gc.ca/eic/site/062.nsf/eng/00120.html [https://perma.cc/KWK5-7ACQ].

also recognizing a need to promote electronic commerce. The Nigerian approach to data protection does not appear to have a definitive approach, and as a result, many of the GDPR principles are replicated without fitting into the local context. Online lenders, for example, have made it common practice to send messages to the contacts of customers who default on their loans. Customers usually agree in this case to allow access to their phone contacts and for such messages to be sent. Most of the people targeted here are illiterate and unable to comprehend what they have agreed to. As a result, concerns about how to obtain consent from customers who may not understand privacy policies must be addressed in a Nigerian data protection law.[480] I argue that Nigerians are becoming more aware than ever before that, technological advancements are posing a greater threat to information privacy, but are unsure how to protect their personal data, particularly in the absence of a clearly defined legal framework that reflects their immediate data protection concerns. As a result, insights from the evolution of the Canadian data protection framework and the drafting of PIPEDA can help policymakers in Nigeria develop a data protection legislation that balances competing interests while also reflecting the country's social, economic, and political realities.

With respect to the adequacy criteria, Canada has consistently received high marks for factors such as respect for the rule of law and fundamental rights, which contributed to a positive adequacy decision. Furthermore, the issue of access to European personal information for national security purposes was never considered when the original adequacy regime was developed, and when the adequacy decision was made in 2001. However, the Canadian government has taken a proactive approach by establishing the NSIRA to provide evidence of necessity and proportionality in such data collection. It is submitted that this structure acknowledges the need for this balance and provides important lessons for any jurisdiction the establishment of an independent

480 Sami Tunji, "FG Probes online banks over breach of customers data privacy" (25 January 2022), Online: *Punchng.com* <https://punchng.com/fg-probes-online-banks-over-breach-of-customers-data-privacy/> [https://perma.cc/87VM-35NP].

supervisory authority. Canada also actively contributes to the development of international data protection standards, and its data privacy framework is heavily influenced by these standards.

The Canadian data protection framework is clearly not perfect, but there is a strong commitment to ensuring that it meets international standards. It is also clear that, despite being somewhat out of date, the structure of the privacy framework remains very relevant today and provides significant lessons for jurisdictions such as Nigeria. In the following Chapter, I summarize the dissertation's findings and make recommendations for developing a comprehensive data protection framework for Nigeria.

CHAPTER 5: SUMMARY AND RECOMMENDATIONS

5.1 Research Findings

The primary objective of this dissertation is to evaluate the "adequacy" of Nigeria's data protection frameworks. Given that there are no unilaterally internationally agreed standards of data protection, an assessment of Nigeria's adequacy is made within the framework of the requirements of the European Commission, whose regulation, the GDPR, Bennett refers to as the most ambitious and comprehensive data protection regulation in the world.[481] This assessment criterion is embedded in the provisions of Article 45(2) of the GDPR that assess whether a third country has an adequate framework that allows European data subjects' data to be securely transferred to such country.

The dissertation aimed to answer three important questions in determining the adequacy of the Nigerian data protection framework. Firstly, I determined what role the "adequate protection" criteria provided in Section 45(2) of the GDPR plays in establishing an international framework for personal data protection. Secondly, I asked that if an application were made to the EC based on the existing assessment criteria, would Nigeria be able to secure a positive adequacy assessment. I then go on to ask what lessons Nigeria can learn from Canada, which has received an EC adequacy decision. In answering these questions, I identified three major findings based on my evaluation of the Nigerian data protection framework within the Article 45(2) GDPR framework and comparative analysis of the Canadian data protection framework.

In identifying the first key finding, this dissertation establishes that the GDPR is currently the most comprehensive data protection legislation in the world, and that due to the lack of an

[481] Bennett, *supra* note 92 at 240.

omnibus international data protection framework, as well as the GDPR's extraterritorial application to other countries, it has come to play a prominent role in setting international standards. I also contend that the Article 45(2) adequacy assessment criteria provide a good starting point for countries such as Nigeria to assess their data protection framework, particularly because it provides a broader assessment criterion that challenges the widely held belief that the existence of data protection legislation is adequate to determine the existence of a comprehensive data protection framework. However, as a cautionary note, I identify that while Article 45(2) GDPR provides a strong assessment criterion in theory, in practice other extrinsic factors such as a third country's political and economic relationship with the EU are considered, and the absence of an adequacy decision does not imply that a country's data protection framework is inadequate.

Secondly, based on the assessment conducted in this dissertation, I find that Nigeria's data protection framework as presently constituted is inadequate for several reasons. I establish that one of the primary reasons for this is that data protection as a concept is relatively new in the country, and policymakers in attempting to develop a framework for Nigeria have largely replicated European standards without considering specific domestic challenges that may necessitate legislation that specifically addresses these issues. Furthermore, Nigeria appears to have fallen into the same trap in developing its data protection framework by introducing legislation without considering other factors that establish an adequate data protection framework. One major impediment here is the disregard for the rule of law and willful violation of the fundamental rights of citizens, which provides a clear indicator of the level of respect for data protection principles, which is also a right. Other evident limitations identified include the overall impact of the NDPR developed by NITDA, which is a subsidiary legislation developed by a regulator which has questionable and at best limited authority to regulate data protection Nigeria.

The lack of a redress mechanism for data subjects, and the failure to establish an independent supervisory authority has made the implementation of existing data protection regulations and principles difficult. Perhaps the failure to domesticate international treaties to which Nigeria has committed itself is the clearest indicator of the value Nigeria currently places on personal data protection. As a result, while progress has been made, I argue that much more work remains to be done to establish an adequate data protection framework for Nigeria.

Thirdly, while assessing Canada's data protection framework, I discovered that, while Canada's PIPEDA is currently considered outdated and in need of reform to conform to modern realities, the structure of the Canadian framework in terms of the establishment of an independent supervisory authority, effective redress mechanisms, and commitment to international obligations provides valuable lessons for countries such as Nigeria. A key finding is that Canada's data protection framework was developed through extensive consultation and was modeled to fit their economic, political, and social realities, and that replicating legislation from other jurisdictions cannot replace the work required to develop a data protection framework that addresses domestic data protection concerns. While there are obvious challenges in adhering to the rule of law, respect for fundamental rights, and access to personal data for personal security purposes, I find that the existence of independent institutions that are largely free of executive influence, as well as the creation of oversight mechanisms such as the NSIRA, has been instrumental in Canada maintaining high marks on various rule of law indexes.

Overall, I find that even though Nigeria has made no attempt to obtain an EU adequacy decision, the GDPR has influenced the development of data protection regulations in Nigeria. Nigeria has also incorporated adequacy provisions into its own regulations, indicating that it is aware of the standards but appears to have made no attempt to comply with them. As previously

stated, I argue that, while obtaining a positive adequacy decision from the EU is largely determined by the EC's political and economic considerations, such determinations have been largely inconsistent and have not favored African countries. However, the adequacy criteria under Article 45(2) of the GDPR provide a good assessment framework and, as such, if Nigeria is to develop a comprehensive data protection framework, this is a strong or important starting point.

5.2 Recommendations

Following the findings in Chapter three, that there is more work to be done to ensure that Nigeria develops an adequate data protection framework in conformity with the assessment criteria of Article 45(2) GDPR, and taking into account the key lessons learned from an evaluation of the Canadian data protection framework, this dissertation offers seven key recommendations, which are not exhaustive, but, if implemented, will make an important contribution towards establishing an "adequate" data protection framework in Nigeria.

5.2.1 Strengthening the Rule of Law and Accountability for Human Rights

The rule of law and accountability for human rights are critical for establishing and maintaining good governance systems and achieving inclusive development. More importantly, for the purposes of this dissertation, adherence to the rule of law and respect for fundamental human rights is a necessary precondition for the establishment of a framework capable of adequately protecting citizens' personal data. Fundamentally enhancing data protection in Nigeria will require a commitment by the government to holding public and private institutions and entities accountable to laws that are promulgated publicly, equally enforced, independently adjudicated, and consistent with international human rights norms and standards. This will necessitate the strengthening of an independent judiciary as well as ensuring compliance with judicial pronouncements.

It is noted however that achieving this will require a significant change to governance systems in Nigeria. Perhaps policymakers, data protection scholars, and civil society organizations can contribute to the call for Nigeria to adhere to the rule of law and fundamental rights by setting the agenda for future administrations and identifying these considerations as critical for Nigeria's data protection framework to be considered adequate under international standards, as well as the potential economic benefits to the country.

5.2.2 Establishment of Oversight Mechanisms of The Collection of Personal Data for The Purposes of National Security.

The lack of an adequate oversight mechanism that governs the access of security and public officials to access personal data for national security purposes in Nigeria is concerning. It is also recognized that there is an overarching need for such data collection. However, as highlighted in this dissertation, unrestricted access to personal data by public officials is a major concern for European officials. It is recommended that the laws that guarantee access to personal data for security purposes be properly identified and streamlined, and that such laws be amended as necessary to reflect the need for necessity and proportionality in public authorities accessing personal data for national security purposes. I also advocate for the establishment of an independent oversight mechanism or institution. This could include establishing a body that supervises the adherence of public authorities to statutory requirements and conducts reviews to ensure that the personal data of citizens is not accessed arbitrarily for national security purposes.

5.2.3 Enacting A Comprehensive Homegrown Data Protection Legislation

As previously stated, Nigeria's current data protection legislation is a subsidiary legislation developed by a government agency without legislative oversight or approval. The World Bank correctly described the regulation as a stopgap measure.[482] As a result, if Nigeria wants to develop

[482] World Bank, supra note 340.

a comprehensive data protection framework, it needs to start with a comprehensive Act. Since NITDA's introduction of the NDPR, the Digital Identity Ecosystem Legal and Regulatory Reform Working Group has made a concerted effort to present a data protection bill for public comment, which has elicited comments from stakeholders to strengthen the bill.[483] However, it appears that a decision has been made to go back to the drawing board, as the NIMC has published a request for a consultant to develop a new Bill as well as other regulations to support the bill.[484]

I recommended that the new data protection bill that is drafted should jettison the NDPR as a starting point and ensure that the provisions of the new Bill fit the Nigerian context of what data protection is. In terms of the proposed legislation's content, it was determined that some provisions of the NDPR such as the extraterritorial provisions which were retained under the Bill create enforcement concerns and are unimplementable. Drafters of the new Bill must avoid the temptation of simply copying the GDPR verbatim, but instead conduct comparative studies of the approach of jurisdictions which have similar circumstances with Nigeria and look to standards developed by Ecowas and the African Union to develop a solution that works for Nigeria. I further recommend that the starting point should be an identification of the fundamental basis for data protection in Nigeria, where drafters can take into consideration the attitude of Nigerians to data protection, specific data protection concerns and enforcement measures that, if applied, will alleviate these concerns. Preferably, this presents an opportunity for Nigeria to establish a truly homegrown data protection framework that can be replicated in Sub-Saharan Africa.

The development of comprehensive data protection legislation can only be accomplished through thorough and wide-ranging consultation. It is important to emphasize that such important

---

483 Scott, *supra* note 235.

484 Tosin Omoniyi, "Data Protection: Indignation as FG Abandons Draft Bill, seeks 'Consultants' for Fresh Process" (November 17, 2021) online: premium times <https://www.premiumtimesng.com/news/top-news/495768-data-protection-indignation-as-fg-abandons-draft-bill-seeks-consultants-for-fresh-process.html>. [permalink: https://go.exlibris.link/Mlhg9lss]

legislation should not be drafted hastily or in silos. To assist policymakers in developing such legislation, a detailed analysis of the identified legal basis for the processing of personal data in Nigeria must be conducted. This process must also identify and engage relevant stakeholders, which will include lawyers, policy experts, operational consultants, public and private sector organizations, civil society organizations, and national security officials. This broad consultation will ensure that various elements are captured and will aid in the development of a truly Nigerian data protection law. This is similar to the approach taken in the drafting of Canada's PIPEDA and its most recent data protection bill, Bill C-11.

5.2.4 Establishment of An Independent Data Protection Authority

One of the most obvious flaws in Nigeria's current data protection framework is the lack of an independent supervisory authority. The NITDA, which currently oversees the implementation of the NDPR, is an arm of the Ministry of Communication and Digital Economy, and by virtue of the NITDA Act is subject to the minister's whims and caprices. Nigeria, requires an independent Data Protection Authority (DPA) for a variety of reasons, including ensuring that it meets international data protection standards and having a dedicated body with the necessary expertise and skills to ensure that data subject rights are effectively developed. The proposed Data Protection Bill 2020 acknowledged the need for a DPA, but reviews of the Bill show that certain provisions need to be improved to ensure its independence.[485]

I recommended that the DPA's independence be a focal point in the provisions made for its enactment, and that other legislation establishing independent agencies, such as the Economic and Financial Crimes Commission (EFCC) and the Independent Corrupt Practices and Other Related Offences Commission (ICPC), be consulted to determine the appropriate framework to be

[485] Scott, *supra* note 235.

adopted. The contemplated legislation must clearly identify a proper structure for appointment and provide security of tenure for members of the DPA. The legislation must also specify how and on what grounds members of the DPA can be removed. The qualifications required for appointment as a member of the DPA should also be clearly stated. This should include proof of data protection expertise as well as membership in organizations of certified professionals.

It should be noted that, unlike the Canadian OPC, which is guaranteed a level of independence due to its status as an Office of Parliament, the independence of government agencies in Nigeria can be difficult to achieve. One major reason for this is the funding of ostensibly independent agencies. Due to funding constraints, organizations that are legally mandated to be independent are subject to executive control. A possible solution might be granting the supervisory authority the power to generate its own revenue through fines and administrative fees and use that revenue for its own purposes. However, it is important to ensure that the powers to impose fines and the limits of such fines should be clearly spelt out in the enabling legislation of the DPA. The powers of the DPA to regulate other government agencies must also be emphasized. This is critical because if the DPA is not perceived to have such supervisory authority, it may be difficult to regulate public bodies.

5.2.5 Developing and Promoting Effective Redress Mechanisms

Since the implementation of the NDPR, there has been no clear framework for effectively enforcing data subjects' rights, as NITDA has failed to establish an administrative redress panel and a clear pathway for data subjects to judicially enforce their rights. First, the data protection legislation that is developed should clearly define the appropriate redress mechanisms available to data subjects. This should cover the steps to take before filing a formal complaint with the supervisory authority. The DPA should be given the authority to establish an administrative redress panel, which would be responsible for resolving complaints, resolving data subject-organization

disputes, and issuing complaint orders, among other things. Such a redress mechanism must adhere to fundamental rights principles by ensuring that the ARP is impartially formed and that parties are afforded an opportunity for proper representation and a fair hearing.

The judiciary also has a role to play in ensuring that the DPA's activities are properly supervised. It is recommended, however, that where a data subject believes his right has been violated, filing a complaint with the DPA be considered a condition precedent to cases being heard by the court. The rationale is to ensure that a defined process for seeking redress exists, as well as to prevent an already overburdened judicial system from being overwhelmed by a flood of data protection cases. The DPA's resolution of data protection cases should also be time-bound, so that if a case is not resolved within a certain time frame, a data subject may be able to seek redress in court. This will also ensure that the enforcement of data privacy rights is not hampered by bureaucratic restrictions.

5.2.6 Determination of The Enforcement Model and The Scope of The Enforcement Powers

The enforcement model to be implemented under the Nigerian data protection framework must be properly defined and determined. The EU and Canada have used different enforcement methods, with the EU insisting on imposing administrative penalties and the Canadian OPC having limited powers to issue administrative penalties. It is also established that where fines are permissible under the Canadian model, such fines are limited. In this context, Nigeria can choose from several models for determining how data protection can be enforced within its borders. It is recommended that the enforcement model cover both the private and public sectors effectively. While fines may be applicable to private sector organizations, imposing fines on public bodies may be difficult, and thus the means to ensure compliance by public bodies should be properly identified.

It is important to note that there has been a push recently for countries to adopt a strict enforcement regime that includes imposing large fines, and it is recommended that Nigeria follow suit. Nigeria may also take other enforcement measures, such as ordering such organizations to stop processing personal data for a set period and fines must be subject to judicial oversight, following the EU model. It is also suggested that Nigeria would be best served by granting the DPA the authority to impose fines and other enforcement measures. In reaching this conclusion, the lengthy delays that characterize court cases in Nigeria are considered and, as a result, giving the court enforcement powers may hamper its effectiveness.

5.2.7 Taking A Lead Role in The Development of Data Protection Standards on The Continent and Participating in International Data Protection Frameworks

Nigeria, as the most populous country in Sub-Saharan Africa and a leader in the developing digital economy, must play an important role in the development and refinement of an African data protection framework. This framework already exists through the Ecowas Supplementary Act on Personal Data Protection and the African Union Malabo Convention, but several countries, including Nigeria, have not domesticated, or implemented it.

Nigeria also stands to gain a lot from participating in data protection frameworks at an international level. As previously stated, Canada has contributed to the development of OECD and APEC data protection frameworks, which has influenced the development of its own data protection legislation. The ratification of the Convention 108 by Nigeria is one way the country can participate at the international level. This will demonstrate Nigeria's commitment to the development of data protection within the country and, as specified by the EC, will be advantageous if Nigeria intends to seek an adequacy decision from the EU.

With the impending implementation of the African Continental Free Trade Area Agreement (AfCFTA), the issue of Pan-African data protection legislation will once again be

raised. Nigeria's status may provide impetus for other African countries to develop their own data protection regulations, as well as lead to standardization across Africa.

5.3 Concluding remarks

The main objective of this dissertation was to determine whether Nigeria's data protection framework was adequate considering the GDPR's emerging international standards. The framework established by Article 45 (2) of the GDPR was used to determine adequacy. As shown in the findings of the evaluation, Nigeria will need a lot of work to meet the European adequacy standard. While Nigeria has not sought an adequacy decision, it is important to recognize that international standards have influenced the country's approach to data protection. I must also emphasize that by advocating for the development of an adequate framework for the protection of personal data in Nigeria, I am advocating for improvements that go beyond the scope of Nigeria's current approach to data protection reforms. I maintain that Nigeria's data protection framework cannot be considered adequate unless there is substantial adherence to the rule of law, respect for fundamental rights, and restrictions on access by public authorities to personal data.

Furthermore, I do not overlook concerns that the GDPR's extraterritorial provisions may amount to data imperialism. This necessitates that, in developing its data protection framework, Nigeria must look beyond the standard set by the GDPR, as it is necessary to develop data protection legislation and framework that reflect unique socio-economic realities. Socio-economic realities in this context tie in with Mannion's observation that lack of technological expertise and increased cost associated with compliance with regulatory compliance may create negative impacts if the GDPR is wholly adopted by African countries.[486] I also emphasize that this approach should aim to balance competing interests by ensuring that the legislation created does not add an

[486] Mannion, *supra* note 37 at 710

unnecessary layer of regulation that stifles innovation while also protecting the fundamental rights of its citizens.

BIBLIOGRAPHY

LEGISLATION

INTERNATIONAL TREATIES

APEC, Digital Economy Steering Group Privacy Framework, APEC#217-CT-01.9 (2015).

Convention on Cyber Security and Personal Data Protection, African Union, June 27, 2014.

Convention on the Protection of Individuals with Respect to Automatic Processing of Personal Data, 28 January 1981, ETS 108 (Entered into force 1 October 1985).

EC, Consolidated Version of the Treaty on European Union, (2008) OJ L 115/13.

OECD, Council of the OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980).

Supplementary Act on Personal Data Protection within ECOWAS, 16th February 2010, A/SA.1/01/10.

U.N. General Assembly resolution 2200A (XXI) of 16th Dec. 1966; in force 23rd March 1976.

United Nations (U.N.) General Assembly resolution 217 A (III) of 10th Dec. 1948.

CANADA

Anti-terrorism Act, 2015 S.C. 2015, c. 20.

Canadian Charter of Rights and Freedoms, s 7, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

Privacy Act R.S.C., 1985, c. P-21.

Conflict of Interest Act, SC 2006, c 9.

Personal Information Protection and Electronic Documents Act, SC 2000, c.5.

Canadian Security Intelligence Service Act R.S.C., 1985, c. C-23.

Communications Security Establishment Act S.C. 2019, c. 13.

National Security Act, 2017, SC 2019, c. 13

National Security and Intelligence Review Agency Act S.C. 2019, c. 13.

National Security and Intelligence Committee of Parliamentarians Act, S.C. 2017, c. 15.

Digital Privacy Act (S.C. 2015, c. 32).

EUROPEAN

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to processing of personal data and on the free movement of such data, 24 October 1995, OJ L 281/31.

EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council 2016/679 of 27 April 2016 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*) [2016] OJ, L 119/1 p. 1-88. (Entered into force 25 May 2018).

NIGERIAN

Constitution of the Federal Republic of Nigeria, LFN 1999 as amended c.23.

Cybercrimes (Prohibition, Prevention, Etc) Act, 2015.

Lawful Interception of Communications Regulations 2019

Mutual Assistance in Criminal Matters Act 2019.

National Information Technology Development Agency Act, LFN 2007, c.28.

Nigerian Communications (Enforcement Process, etc.) Regulations 2019, B 82.

Nigerian Communications Commission Act, LFN 2003, N.9.

Nigerian Data Protection Regulation, 25th January 2019.

Nigerian Data Protection Regulation: Implementation Framework.

Same Sex Marriage (Prohibition) Act, 2013.

Terrorism Prevention Act (TPA), 2013 as amended Gazette A27.

JURISPRUDENCE

CANADA

A.T. v. Globe24h.com, [2017] 4 FCR 310.

Canada (Privacy Commissioner) v. Blood Tribe Department of Health, [2008] 2 SCR 574.

R v Spencer, [2014] SCC 43.

Re Manitoba Language Rights [1985] 1 SCR 721.

Reference re Secession of Quebec, [1998] 2 S.C.R. 217.

Rodgers v. Calvert, 2004 CanLII 22082 (ON SC).

Roncarelli v. Duplessis, [1959] S.C.R. 121.

EUROPEAN

Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, C-311/18 [2020] ECR.

Digital Rights Ireland Ltd and Kärntner Landesregierung and Others, C-293/12 & C-594/12, [2014] ECR.

European Commission v Federal Republic of Germany, C-518/07 [2010] ECR at 4.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, C-131/12, (2014) ECR I-1.

Schrems v Data Protection Commissioner (2015) ECJ, ECLI:EU:C:2015:650.

NIGERIA

Attorney-General of Lagos State v. Attorney-General of the Federation (2002) 1 WRN 1.

Emerging Market Telecommunication Services v Barr Godfrey Nya Eneye (2018) LPELR-46193.

Incorporated Trustees of Digital Lawyers Initiative (on behalf of data subjects whose personal data were exposed by the Unity Bank Plc) v. Unity Bank Plc (Unreported) Suit No: FCH/AB/CS/85/2020.

Incorporated Trustees of Digital Lawyers Initiative v. LT Solutions & Multimedia Limited (Unreported) Suit No: HCT/262/2020

Lakanmi Vs. A-G. Western Region (1974) EGSLR 713.

Ondo State University v Folayan (1994) 7 & 8 SCNJ (PT.1).

ECOWAS

Dasuki v Federal Republic of Nigeria (2016) ECOWAS CJ, ECW/CCJ/JUD/23/16.

SECONDARY SOURCES

BOOKS

Adejumobi Said, *Governance and Politics in Post/Military Nigeria: Changes and Challenges* (New York: Palgrave Macmillan, 2011).

Agbali Mohammed et al, *Data Privacy and Protection: The Role of Regulation and Implications for Data Controllers in Developing Countries* (Cham: Springer International Publishing, 2020).

Bayley Robin and Colin Bennett, *Privacy Impact Assessments in Canada* in David Wright and Paul de Hert, *Privacy Impact Assessment* (New York; Springer 2012).

Bennett Colin & Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (New York, NY: Routledge, 2018).

Bieker Felix, *Enforcing Data Protection Law – the Role of the Supervisory Authorities in Theory and Practice* (Cham, Springer International Publishing, 2017).

Bradford Anu, *The Brussels Effect: How the European Union Rules the World* (New York, NY: Oxford University Press 2020).

De Hert Paul & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action* (Dordrecht: Netherlands, Springer 2009).

Borrows John, *Canada's Indigenous Constitution* (Toronto, University of Toronto Press, 2010).

Kuner Christopher, *Transborder Data Flows and Data Privacy Law* (Oxford; Oxford University Press, 2013).

Lindsay David, *The Role of Proportionality in Assessing Trans-Atlantic Flows of Personal Data* (Antwerp, Belgium: Intersentia 2017).

Makulilo Alex, *The Future of Data Protection in Africa*, *in* Alex B. Makulilo, *African data Privacy laws* (Cham, Springer International Publishing, 2016).

Voigt Paul & Axel von dem Bussche, *The EU General Data Protection Regulation* (New York, NY: Springer 2017).

Werro Franz, *The Right to be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia* (Cham: Springer International Publishing, 2020).

ARTICLES AND JOURNALS

Abdulrauf Lukman, & Charles Fombad. “Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms” (2017) 38:2 Liverpool L Rev 105-134.

Abdulrauf Lukman, The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa (PHD Dissertation, University of Pretoria, 2015) [Unpublished].

Akanbi Mohammed & Ajepe Shehu, “Rule of Law in Nigeria” (2012) 3:1 Journal of Law, Policy and Globalization 1-9.

Anyim Wisdom, “Twitter Ban in Nigeria: Implications on Economy, Freedom of Speech and Information Sharing.” (2021) 5975 Library Philosophy and Practice 1-14.

Azzi Adele, “The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation” (2018) 9:2 Journal of Intellectual Property, Information Technology and E-Commerce Law 126-137.

Babalola Olumide, “Nigeria’s data protection legal and institutional model: an overview” (2021) 0:0 International Data Privacy Law 1-9.

Bennett Colin & Charles Raab, “The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response” (1997) 13:3 The Information Society 245-263.

Bennett Colin, “Adequate Data Protection by the Year 2000: The Prospects for Privacy in Canada” (1997) 11.1 International Review of Law, Computers & Technology 79-92.

———, “Is Canada Still ‘adequate Under the New European General Data Protection Regulation?” (8 August 2016), Online: colinbennett.ca, <https://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-new-general-data-protection-regulation/> [https://perma.cc/7KQG-9ZGA].

———, “The Council of Europe’s Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession” (2020), online: Center for International Governance Innovation https://www.cigionline.org/publications/council-europes-modernized-convention-personal-data-protection-why-canada-should/ [https://perma.cc/FB9C-54NT].

———, “The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?” (2018) 23:2 Information Polity 239-246.

———, “The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas” (2003) 46:2 Canadian Public Administration 218-242.

Bergman Gwyneth & Emmett Macfarlane, “Protecting Privacy? Government and Parliamentary Responsiveness to the Privacy Commissioner of Canada” (2021) 64:3 Canadian Public Administration 437-456.

Bloodworth Michelle et al, “The Rule of Law in Canada: A Global Template?” (2013) 31:2 National Journal of Constitutional Law 111.

Blume Peter, “Transborder Data Flow: Is there a Solution in Sight?” (2000) 8:1 International Journal of Law and Information Technology 65–86.

Bygrave Lee, “Privacy Protection in a Global Context—A Comparative Overview” (2004) 47:1 Scandinavian Studies in Law 319-348.

Curtiss Tiffany, “Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies” (2016) 12:1 Washington Journal of Law, Technology & Arts 96-122.

De Hert Paul & Michał Czerniawski, “Expanding the European data protection scope beyond territory: Article 3 of the general data protection regulation in its wider context” (2016) 6:3 International Data Privacy Law 230-243.

Duque de Carvalho Sara, “Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108” (2019) 5:1 European Data Protection Law Review 54-64.

Fowowe Solomon, “Buhari Declines Assent to Digital Rights Bill, Four Others”, (20 March 2019), online: AllAfrica.com <https://go.exlibris.link/0Gx1975y>.

Goddard Michelle, “The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact” (2017) 59:6 International Journal of Market Research 703-705.

Greenleaf Graham, “Global Data Privacy Laws 2019: New Eras for International Standards” (2019) 157:1 Privacy Laws & Business International Report 1-4.

———, “Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance” (2021) 169:1 Privacy Laws & Business International Report 3-5.

———, “Nigeria regulates Data Privacy: African and Global Significance” (2019) 158 Privacy Laws & Business International Report 1-4.

Hondius Frits, “A Decade of International Data Protection” (2009) 30:2 Netherlands International Law Review 103-128.

Iruoma Kelechukwu, “Privacy Concerns Hobble Nigeria’s Digital ID Push” (August 2 2021), Online: AllAfrica.com <https://go.exlibris.link/1qdz3x3v>

Iwobi Andrew, “Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime”' (2016) 26:1 Transnational Law & Contemporary Problems 14-59.

Iwuoha Chidubem, and Ernest Aniche, “Protests and blood on the streets: repressive state, police brutality and #ENDSARS protest in Nigeria.” (2021) 34:3 Security Journal 1-23.

Kirby Michael, “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy” (2011) 1:1 International Data Privacy Law 6-14.

Koutrous Nicholas and Julien Demers, “Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement” (2013) 11:1 CJLT 79.

Kuner Christopher, “An International Legal Framework for Data Protection: Issues and Prospects” (2009) 25:4 The Computer Law and Security Report 307-317

———, “Data Protection Law and International Jurisdiction on the Internet (Part 1)” (2010) 18:2 International Journal of Law and Information Technology 176-193.

———, “The Internet and the Global Reach of EU Law” (2017) LSE Legal Studies Working Paper No. 4.

Levin Avner & Mary Jo Nicholson, “Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground” (2005) 2:2 U Ottawa L & Tech J 357.

Makulilo Alex, “Data Protection Regimes in Africa: Too Far from the European Adequacy' Standard?” (2013) 3:1 International Data Privacy Law 42-50

———, “Nigeria’s Data Protection Bill: Too many surprises” (2012) 120:1 Privacy Laws & Business International Report 24-27.

———, “The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius” (2020) 25:1 The International Journal of Human Rights 117-146.

Mannion Cara, “Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets” (2020) 53:2 Vanderbilt Journal of Transnational Law 685-711.

Marczak Bill et al, “Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles” (1 December 2021), Online: The Citizen Lab <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/> [https://perma.cc/7SLM-AW3G].

Nesbitt Michael, “Reviewing Bill C-59, an Act Respecting National Security Matters 2017: What’s New, what’s Out, and what’s Different from Bill C-51, A National Security Act 2015?” (2020) 13:12 School of Public Policy Publications 1-33.

Niebel Crispin, “The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy” (2021) 40:4 The Computer Law and Security Report 1 -15.

Ogala Emmanuel, “Exclusive: Jonathan Awards $40 Million Contract to Israeli Company to Monitor Computer, Internet Communication by Nigerians” (25 April 2013), Online: Premium Times, https://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-toisraeli-company-to-monitor-computer-internet-communication-by-nigerians.html [https://perma.cc/TE3F-FJ9X].

Okon Elijah, "The Rule of Law in Nigeria: Myth or Reality" (2011) 4:1 J Pol & L 211.

Oloyede Ridwan, “Surveillance Law in Africa: A Review of Six Countries Nigeria Country Report” (21 October 2021), Online: ids.ac.uk <https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Nigeria%20Country%20Report.pdf?sequence=7&isAllowed=y> [https://perma.cc/8H2J-TQ4P].

Omoniyi, Tosin, “Data Protection: Indignation as FG Abandons Draft Bill, seeks 'Consultants' for Fresh Process” (17 November 2021), online: premium times <https://www.premiumtimesng.com/news/top-news/495768-data-protection-indignation-as-fg-abandons-draft-bill-seeks-consultants-for-fresh-process.html>. [permalink: https://go.exlibris.link/Mlhg9lss].

Orkin Andrew, “When the Law Breaks Down: Aboriginal Peoples in Canada and Governmental Defiance of the Rule of Law” (2003) 41:3 Osgoode Hall LJ 445.

Parsons Christopher &Adam Molnar, “Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports” (2018) 16:1 CJLT 144.

Parsons Christopher, “Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance” (2015) 3:3 Media and communication 1-11.

Salami Emmanuel, “Nigerian Data Protection Law: The Effectiveness of the Nigerian Data Protection Bill as a Tool for Fostering Data Protection Compliance in Nigeria” (2019) 43:9 Datenschutz und Datensicherheit 575-582.

Sanni Kunle, “Despite Promising Rule of Law, Bawa’s EFCC Sticks to Crude Tactics of Hotel, Home Invasions” (9 October 2021), Online: Premium Times <https://www.premiumtimesng.com/news/top-news/488886-despite-promising-rule-of-law-bawas-efcc-sticks-to-crude-tactics-of-hotel-home-invasions.html>[https://perma.cc/LMR7-PWWJ].

———, “Investigation - how Digital Loan Providers Breach Data Privacy, Violate Rights of Nigerians” (December 10, 2021) Online: Premiumtimes.ng. https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html [Permalink:https://go.exlibris.link/LLkD5VDH]

Scott Bisola & Sandra Eke, “NITDA’s power to regulate non-electronic data” (10 July 2020), Online: Mondaq Business Briefing <https://www.mondaq.com/nigeria/privacy-protection/961436/nitda39s-power-to-regulate-non-electronic-data> [https://perma.cc/PFF4-Q9N2].

Scott Bisola, “A Review of the Nigerian Data Protection Bill 2020” (8 September 2020), online: Mondaq Business Briefing. link.gale.com/apps/doc/A634806812/ITBC?u=uvictoria&sid=summon&xid=8e7f1f2e. [permalink: https://go.exlibris.link/Zfs2JWgD].

Shuaib Musa, “The Changing Pattern of International Trade: Import Substitution Policy and Digital Economy in Nigeria. A Review” (2020) 6:4 International Journal of Economics and Business Management 13-25.

Stoddart Jennifer, Benny Chan, & Yann Joly “The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research” (2016) 44:1 Journal of Law, Medicine & Ethics 143-155.

Suda Yuko, “Japan’s Personal Information Protection Policy Under Pressure” (2020) 60:3 Asian survey 510-533.

Taylor Richard, “Data Localization: The Internet in the Balance” (2020) 44:8 Telecommunications policy 1-15.

Tunji Sami, “FG Probes online banks over breach of customers data privacy” (25 January 2022), Online: *Punchng.com* <https://punchng.com/fg-probes-online-banks-over-breach-of-customers-data-privacy/> [https://perma.cc/87VM-35NP].

Vanberg Aysem, “Informational privacy post GDPR – end of the road or the start of a long journey?” (2021) 25:1 The International Journal of Human Rights 52-78.

Von Danwitz Thomas, “The Rule of Law in the Recent Jurisprudence of the ECJ” (2014) 37:5 Fordham International LJ 1311-1343.

Wagner Julian, “The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?” (2018) 8 International Data Privacy Law 318-337.

Wang Flora, “Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement” (2020) 33:2 Harvard J Law & Tech 661-690.

Watson Jack, “you don't know what you’ve got 'til it’s gone: the rule of law in Canada” (2015) 52:4 Alberta L Rev 689.

GOVERNMENT DOCUMENTS, REPORTS AND WEBSITES

Canada, Office of the Conflict of Interest and Ethics Commissioner, The Trudeau Report, by Mary Dawson (Ottawa: CIEC, 20 December 2017).

———, Trudeau II Report, by Mario Dion (Ottawa: CIEC, 14 August 2019).

Commission Decision (EC) 2002/2 of 20 December 2001 pursuant to Directive (EC) 95/46 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] OJ L2/13.EC, Conclusions of the Presidency on the European Council in Copenhagen, (1993) C 180/93.

Council of Europe, “Chart of Signatures and Ratifications of Treaty 108” (2 December 2021), Online: coe.int <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty treaty num=108> [https://perma.cc/VN9Q-LZ29].

Daniel Therrien, “From State Surveillance to Surveillance Capitalism: The Evolution of Privacy and The Case for Law Reform - Office of The Privacy Commissioner of Canada” (16 June 2021), Online: Priv.gc.ca, <https://www.priv.gc.ca/en/opc-news/speeches/2021/sp-d_20210616/> [https://perma.cc/Z7VH-PKE9].

———, “Op-Ed: Privacy Commissioner Raises Concerns About Bill C-51 - Office Of The Privacy Commissioner Of Canada” (6 March 2015), Online: Priv.gc.ca, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2015/oped_150306/ [https://perma.cc/A2X5-DLSB].

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and

Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", (2011) OJ, C 181/01.

Elizabeth Denham, 'Commissioner's Findings - PIPEDA Case Summary #2009-008: Report of Findings: CIPPIC V. Facebook Inc. - Office of The Privacy Commissioner of Canada' (2009) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/> [https://perma.cc/A22N-5QGH].

European Commission, Adequacy decisions (10 April 2021), online: European Commission https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/M2SQ-FYYY].

GDPR Info, Third countries, (10 April 2021), online: GDPR Info https://gdpr-info.eu/issues/third-countries/ [https://perma.cc/FM4S-D6PQ].

Global Privacy Assembly, "Montreux Declaration-The protection of personal data and privacy in a globalized world: a universal right respecting diversities" (2005), online (pdf): <https://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf> [https://perma.cc/YN25-XQGU].

Government Canada, "Bill Summary: Digital Charter Implementation Act, 2020 - Innovation for A Better Canada" (11 November 2020), online: ic.gc.ca https://www.ic.gc.ca/eic/site/062.nsf/eng/00120.html [https://perma.cc/KWK5-7ACQ].

Industry Canada, "Process for the determination of Substantially Similar Provincial Legislation by the Governor in Council," Canada Gazette Part I, August 3 202. 2385-2389.

Innovation, Science and Economic Development Canada, "Sixth Update Report on Developments in Data Protection Law in Canada" (2019), Online: Ic.gc.ca https://www.ic.gc.ca/eic/site/113.nsf/vwapj/SixthUpdateReportonDevelopmentsinDataProtectionLawinCanada_en.pdf/$file/SixthUpdateReportonDevelopmentsinDataProtectionLawinCanada_en.pdf [https://perma.cc/LWP7-RY8R].

Martin Schenin, "Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism" (28 December 2009), Online: ohchr.org <https://www.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> [https://perma.cc/QWJ8-2PYL].

Office of the Privacy Commissioner, "Guidelines for Processing Personal Data Across Borders - Office of The Privacy Commissioner Of Canada" (2009), Online: Priv.gc.ca https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/ [https://perma.cc/Y629-4LJN].

Office of the Privacy Commissioner, "The Case for Reforming the Personal Information Protection and Electronic Documents Act - Office of The Privacy Commissioner of Canada" (May 2013), online: priv.gc.ca <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/> [https://perma.cc/27SH-B24C].

Opinion 1/15 Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data from the European Union to Canada [2017] OJ C 592/1.

Proshare Nigeria, "Yar Adua orders release of Lagos N10.8b council funds", (24 July 2007), online: Proshare https://www.proshareng.com/news/Nigeria-Economy/Yar-Adua-orders-release-of-Lagos-N10.8b-council-funds/2659 [https://perma.cc/4RLA-J3YN]

Public Safety Canada, "Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy" (2012), Online: Publicsafety.gc.ca <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx> [https://perma.cc/86EP-DK3J].

———, "Parliamentary Passage of Bill C-59: The National Security Act, 2017 - Fulfilling Commitments to Address Former Bill C-51: Overview of New Measures" (2019), Online: Canada.ca <https://www.canada.ca/en/public-safety-canada/news/2019/06/parliamentary-passage-of-bill-c-59-the-national-security-act-2017---fulfilling-commitments-to-address-former-bill-c-51overview-of-new-measures.html> [https://perma.cc/HVK4-YLSL].

Software world, "Number of GDPR Fines Surge by 113% in a Year despite Strict Regulations" (3 October 2021), Online: Software World https://link.gale.com/apps/doc/A674513635/ITBC?u=uvictoria&sid=summon&xid=102f8cb8 [Permalink: https://go.exlibris.link/JFL92XC8].

Standing Committee on Access to Information, Privacy and Ethics: Parliament. House of Commons, "Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act: Report of the Standing Committee on Access to Information, Privacy and Ethics" (Ottawa, Standing Committee on Access to Information, Privacy and Ethics, 2018).

T-CY Committee, "Nigeria Invited to Join the Budapest Convention on Cybercrime" (11 July 2017), Online: coe.int <https://www.coe.int/en/web/cybercrime/-/nigeria-invited-to-join-the-budapest-convention-on-cybercrime> [https://perma.cc/SY87-RJH6].

U.S Department of State, 2020 Country Reports on Human Rights Practices: Nigeria (30 March 2021), Online: State.gov https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/nigeria/ [https://perma.cc/PF93-3C9D].

World Bank, "Nigeria Digital Economy Diagnostic Report" (2019), Online: worldbank.org, https://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf [https://perma.cc/B49K-KZDA].

World Justice Project, "WJP Rule of Law Index- Canada" (2021), Online: Worldjusticeproject.org, <https://worldjusticeproject.org/rule-of-law-index/country/Canada> [https://perma.cc/Y2F7-44DC].

Working Party 29, Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (2002) OJ, C 5035/01.