ANALYZING SECTION 37 OF THE NIGERIAN CONSTITUTION: A HUMAN RIGHTS PERSPECTIVE ON DATA PROTECTION AND PRIVACY

Bello Aderonke Oluwabukola*

Odusola Josephine Gbemisola**

Umejuru Ozioma Rachael***

Abstract

Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) guarantees the right to privacy, encompassing individual privacy, family life, correspondence and communication. Thus, the protection of data and privacy has become a critical component of this digital age, hence the establishment of the Nigerian Data Act 2023 (NDPA) and the release of the General Application and Implementation Directive (GAID), on 20th March, 2025, to regulate the processing of personal data and privacy in Nigeria. The rapid advancements in technology have made it essential for nations to establish comprehensive legal frameworks to safeguard individuals' sensitive information. This article presents a comparative review of privacy and data protection laws across nine countries-Nigeria, India, the European Union, United Kingdom, Japan, Singapore, South Korea, United States and China.This study ultimately recommends a comprehensive implementation of data protection and privacy awareness to all individuals, companies, stakeholders in Nigeria.

Key-Words: Privacy Rights; Data Protection, Date Privacy; Surveillance; Cybercrime; Technology.

* *LL.B, LLM, BL,* National Judicial Institute Studies Fellow; ronkkybammy@yahoo.com; 07081915752

** *LL.B,BL,* National Judicial Institute, Assistant Research Fellow; odusolajosephine@gmail.com; 08102524473

*** *LL.B, BL*, National Judicial Studies Fellow; umejuruozioma@gmail.com; 08033128017

1. **Introduction**

There was no explicit recognition of the right to privacy during the colonial period in Nigeria, as the legal system was governed by English common law which emphasized public order and discipline above individual freedoms. It was also absent in the 1960 Independence Constitution and the 1963 Republican Constitution of. [1] It was reiterated that the colonial administration in Nigeria consistently prioritized public order over individual liberties, including the right to privacy, emphasizing control and discipline, which contributed to the lack of explicit privacy protections in Nigeria's legal framework during and after colonial rule.[2] The right to privacy was first included in the 1979 constitution, and was retained and strengthened under section 37 of the 1999 Constitution of Nigeria.[3]

Section 37 of the 1999 Constitution of Nigeria guarantees the right to privacy, encompassing individual privacy, family life, correspondence and communication. This provision aligns with the international human rights standards including Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which emphasize protection against arbitrary interference and prioritize liberty and privacy in the exercise of other rights.

This paper examines section 37 of the 1999 constitution of Nigeria, which provides that "Every Person shall be entitled to freedom of thought, conscience and religion, including freedom to change his religion or belief including freedom to change his religion or belief and freedom (either alone or in community with others and in public or private) to manifest and propagate his religion or belief in worship, teaching, practice and observance" While section 37 does not explicitly reference personal data or digital privacy, its broad phrasing encapsulates these concerns in the context of modern technology advancements and widespread digital platform usage. The protection against unauthorized access use, or disclosure of personal information whether in physical or electronic form can be interpreted as an extension of this constitutional right. In this light, the Nigeria Data Protection Act 2023 (NDPA) reinforces the constitutional framework by advancing privacy as a fundamental human right in the digital age.

---

[1] Chinua, A. *African Literature (English)-History and Criticism, African Literature-History and Criticism*. Garden City, N.Y: Anchor Press, p.116.
[2] *Ibid.*
[3] Constitution of the Federal Republic of Nigeria, *1999* (as amended), s.37.

2.The Significance of Section 37 in Safeguarding Data Privacy

The Nigeria Constitution provides for the right to privacy, stating that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications are guaranteed and protected.[4] Section 37 is terse, its implications are vast in terms of the legal recognition of personal security, family life, and private communicatio[5].The Constitution protects the inviolability of the home, which means that people have the right to be secure within their homes against unreasonable searches or invasions by government agents. This protection extends to situations where law enforcement seeks to search a person's home. Such search must be backed by a search warrant issued by a court of competent jurisdiction[6]. A breach of the constitutional right to privacy includes unauthorized entry, search, or surveillance. Section 37 affirm the confidentiality of correspondence, referring to communications between people, existing in both tangible forms like letters and in digital formats such as emails and messages[7].This is especially true today, when digital communication is the order of the day, which provides a strong justification for secure communication in which information should not fall prey to illegal interception by any means.[8]

In addition, the safeguard of telephonic communication ensures that the calls made and received by a person are not subject to monitoring or eavesdropping by any unauthorized individual, including the government.[9] Any interception of communication must be based on prior legal procedures and judicial control. While the Constitution refers to "telegraphic communications" and thus may seem archaic, courts and legal scholars interpret this to include modern forms of electronic communication such as SMS, internet chats, and social media messaging[10]. The Constitution's authors might not have envisioned the technology that exists today, but the courts have embraced a flexible interpretation to keep this right relevant today.[11] Section 37 is enforceable by section 46 of the Constitution. This provision allows anyone who claims that their right has been or is about to be infringed to

[4]*Ibid.*
[5] Babalola, *Privacy and Data Protection Law in Nigeria* (2021).p.64.
[6]Administration of Criminal Justice Act 2015, s.144.
[7]Interpretation Act, Cap 123, Laws of the Federation of Nigeria 2004 (accessed 14 September 2025).
[8]Section 38 of cybercrimes (prohibition, prevention) Act 2015.
[9]*Digital rights lawyers initiative* v *NCC (suit No: FHC/ABJ/CS/30/2020).*
[10] Okediran, M. 'The Interpretation of Privacy Right in Nigeria' *Nigeria Law Journal* (2020) Vol.23(1) 18.
[11]*Ibid.*

approach the High Court for relief[12]. This turns the right to privacy into an actionable right, implying that it can be argued in court and remedies can be sought against the violators. Moreover, the courts have ruled that any evidence obtained in violation of privacy cannot be admitted in court especially where the method employed in obtaining such evidence offends constitutional safeguards[13]. However, the right to privacy under section 37 is not absolute since the Constitution provides for reasonable limitations regarding public safety, public order, public morality, or public health as provided in section 45[14].This implies that the government can restrict this right in exceptional circumstances, for instance during official investigations and matters of national security , however such actions must be lawful and proportionate to the threat addressed[15].

In this contemporary digital age, section 37 privacy rights face new challenges in the form of extensive data collection, surveillance technologies, and cybercrime. Many Nigerians use smartphones and online platforms, which raises issues of data privacy, digital profiling, and unauthorized access to personal information.[16] Acknowledging these issues, Nigeria enacted the Nigeria Data Protection Regulation (NDPR) in 2019 and subsequently the Nigeria Data Protection Act in 2023 to govern the process of collecting, storing, and utilizing personal data. While these laws aim to support the goals of Section 37, they are still in early stages of implementation, and most agencies and businesses remain non-compliant.[17] Moreover, state-sponsored surveillance has been implicated, including spyware and monitoring technologies used often without judicial authorization. Such conduct undermines the very purpose of Section 37 and further diminishes people's confidence in public organizations without adequate control and supervision[18]. Human rights organizations and civil society groups have demanded more transparency, judicial oversight, and an independent privacy commission to enforce these protection.

In conclusion, section 37 of the 1999 constitution protects a vital right that upholds the dignity, freedom, and autonomy of individuals against any unlawful interference[19]. For this right to be relevant in contemporary

[12] Constitution of the Federal Republic of Nigeria 1999 (as amended), s.46.
[13] Evidence Act 2011, s.14.
[14]Constitution of the Federal Republic of Nigeria 1999 (as amended), s.45.
[15]*Ibid.*
[16]Media Rights Agenda, online privacy and Expression in Nigeria, 2021.
[17] Nigeria Data protection Regulation (NDPR),2019, Nigeria Data Protection Act 2023.
[18]SERAP, Surveillance and privacy in Nigeria, 2021.
[19]Constitution of the Federal Republic of Nigeria, 1999 (as amended), s.37.

society, it needs ongoing interpretation to reflect current realities and requires strong legislative and institutional support. Protection of the "home" ensures safety from illegal search or entry or even surveillance imposed by state actors.[20] The word "correspondence" covers letters, emails, text messages and all forms of communication deemed personal in nature. Interception, tapping, or unauthorized listening to 'telephone conversations' is prohibited.[21] While the Constitution refers to 'telegraphic communications,' this term is now given an expansive interpretation that includes contemporary digital and electronic communication technologies used today.[22]

2.1 Context and Intent Behind the Provision

The first express recognition of the right to privacy in the constitutional history of Nigeria appeared in Section 34 of the 1979 Constitution and was carried forward in section 37 of the 1999 Constitution.[23] This was a departure from the 1963 Republican Constitution which did not specifically include the right to privacy. The 1979 Constitution was in part a model of the US Bill of Rights and other international constitutions that focus on the individual's liberty.[24] After civilian rule was restored in 1999, the drafters of the constitution copied much of the rewritten 1979 Constitution word for word including the privacy clause. However, section 37 was expanded, to cover new forms of communication such as "telephone conversations and telegraphic communications," in the light of technological progress in communications.[25]The provision from the 1979 Constitution was largely preserved by the Obasanjo led Constitutional Debate Coordinating Committee (CDCC) in 1998. The provision reflects a conscious direction toward the protection of civil freedoms in the democratic post military state. The paragraph was written to offering constitutional protection to citizens against unjustified state intervention, as occurred during increasing surveillance and arbitrary searches under military rule[26].

The legislative intent behind section 37 was to promote the right to privacy as an aspect of human dignity and integrity by elevating it to

[20]Administration of Criminal Justice Act, 2015, s.144.
[21] The Federal High Court considered the scope of digital rights enforcement in *Digital Rights Lawyers Initiatives v NCC* (FHC/ABJ/CS/30/2020).
[22]C.O. *Constitutional Law in Nigeria* (Evans Brothers, Ibadan 2005).p.170.
[23]The constitution of the federal republic of Nigeria 1979, section 34.
[24]Elias, T.O. *Constitutions and the Rule of Law: A Comparative Study* (Martinus Nijhoff Publishers, 1980) 203–205.
[25]Asein, J.O. *Introduction to Nigerian Legal System* (2nd edn, Ababa Press, 2005) 189.
[26]Report of the constitutional Debate Coordinating Committee (CDCC), Vol.1,1998.

constitutionally guaranteed protection. This provision exemplified Nigeria's embrace of liberal democratic ethos after autocratic military rule, during which civil liberties and human rights were often denied.[27] The drafters of the 1999 Constitution, including the Constitutional Debate Coordinating Committee, built on the experiences from the 1979 Constitution and borrowed from international human rights laws including the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), to domesticate, if not elevate, the right to privacy under the Nigerian constitution.[28]

Common law traditions as well as the international human rights law norms on a global scale –especially Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), not to be subjected to arbitrary intrusion into one's privacy – were sources of inspiration to the Constitution Drafting Committee (CDC) and the Constituent Assembly during pre-1979 constitutional evolution.[29] Even though explicit privacy protections were written into Nigerian constitution for the first time in 1979, the 1999 constitution upheld and reaffirmed this dedication to both personal freedom and privacy, citing their enhanced value in the context of globalization-driven digital times.[30]There was no explicit recognition of the right to privacy in Nigeria's colonial legal system. The legal system was primarily governed by English common law, which focused more on public order and discipline than individual freedoms[31]. Laws were crafted during the colonial era to assert government control over people while rights such as privacy were forfeited to ensure the protection of British administrative interests[32]. The law offered rudimentary protection for privacy rights; these rights were only implicitly recognized through tort law remedies involving acts like trespass to property or defamation, instead of being enshrined as a constitutional right.[33] There was no specific provision for the right to privacy in the 1960 Independence Constitution or in the 1963 Republican Constitution. It took until the

[27]B.O Nwabueze, *'Constitutional democracy in Africa'* (spectrum books, 2003), p147-149.
[28]Odinkalu, C.A. 'The Impact of Economic and Social Rights in Nigeria's Emerging Democracy' *Human Rights Quarterly* Vol.23 No.3 (2001) 555–578.
[29]United Nations Universal Declaration of Human Rights 1948, Article 12, International Covenant on Civil and Political Rights, 1966.Article 17.
[30]Ojukwe, E., "Protection of Privacy under Nigeria Law" (2007) *Nigeria Bar Journal* 33–41.
[31] Asein, J.O. *Introduction to the Nigerian Legal System* (Abuja: NAILS, 2019).
[32] Nwabueze, B.O. *Military Rule and Constitutionalism* (Spectrum Books, 1992) 162.
[33] Okonkwo, C.O. *Tort Law in Nigeria* (Ibadan: Spectrum Books, 2003) 123.

1979 Constitution for there to be an express provision made for the right to privacy in Nigerian constitutional law.

This provision was thus retained and strengthened in section 37 of the 1999 Constitution within the context of a wider commitment to democratic governance and human rights protection.[34] The inclusion of the privacy clause in both the 1979 and 1999 Constitutions was influenced by global human rights developments resulting from Nigeria's membership in the United Nations and the African Union, both of which promote privacy rights.[35] It showed not only an increasing consciousness of personal dignity and autonomy but also the dangers inherent in unchecked state surveillance, particularly after Nigeria's prolonged experience with military rule. The Nigerian legal framework has gradually extended its reach on matters of privacy to issues such as electronic communications and data protection; this is observable in the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015.[36] The Cyber Crimes (Prohibition, Prevention, etc.) Act, 2015, By taking proactive measures, this Act combats identity theft, fraud, and data abuse.[37] It obliges service providers to preserve subscriber information for two years and sanctions its release only under specified situations, including court orders. Furthermore, without a court order, the Act prohibits the unlawful interception of electronic communications for criminal investigations.[38]

The right to privacy is a moving frontier shaped by judicial interpretation, legislation, and advocacy, particularly to ensure Nigerian law aligns with international standards for data protection.[39] Section 37 of the 1999 Constitution emerged from deep legal, historical, and political roots. Professors and scholars have tackled this matter in various ways from mixed reviews both from the critical review and positive review aspect. Ademu-Eteh (2022) criticizes constitutional and statutory provisions in Nigeria intends to ensure data privacy. The author points out that, despite being a basic provision, section 37 of the 1999 Constitution is vague on data processing and does not have the capacity for institutional enforcement in the paper. The paper suggests that the

[34]Constitution of the Federal Republic of Nigeria, 1999 (as amended), s.37.
[35]International Covenant on Civil and Political Rights (ICCPR), Art.17; African Charter on Human and Peoples' Rights, Art.9.
[36]Cybercrimes (Prohibition, Prevention) Act, 2015, ss.37–38.
[37] The Cyber Crimes (Prohibition, Prevention, etc.) Act, 2015. Section 22.
[38]*Ibid.*
[39]Ndubuisi, A. "The Right to Privacy in Nigerian Law" (2020) 25(1) *Nigerian Bar Journal, p* 203.

new laws should include clear definitions and a privacy enforcement agency.[40]

Ogundipe highlights the incompetence of institutions and argues that the absence of special constitutional enforcement makes section 37 largely aspirational. The author clarifies that even the rule-making bodies like NITDA and the NDPC are, in many cases, faced with related issues like limited enforcement powers, unclear responsibilities, as well as inadequate technology infrastructure.[41] Meanwhile, Amah maintains that the acknowledgment of privacy in the 1979 Constitution is a 'constitutional renaissance' as it brought Nigeria's domestic rights framework to the level of at least article 17 of the ICCPR1. He further observes that there remains clear legislative intent in section 37 of the 1999 Constitution to reverse state surveillance during military rule, which had been traditionally accepted.[42] Similarly, Ojukwu also commends the inclusion of "telephonic and telegraphic communications" in Section 37 of the 1999 Constitution and regards it as a forward-looking provision because it recognized the significance of technology and digital rights in contemporary democracies[43].

3.**Definition and Scope of Data Protection and Privacy**

Privacy is the right by which individuals protect their personal lives and information from public scrutiny, interference, and access without consent.[44] It empowers people to govern how their personal information, including data about themselves, communications, and activities, is used, published, and accessed.[45] Data protection laws provide a framework within which personal data may be safely collected, stored, processed, and transmitted.[46] While privacy is broad, data protection as a subset deals specifically with matters relating to handling personal information.[47] Personal data consists of details that identify an

[40] Ademu-Eteh, D., "from text to reality: Evaluating section 37 and Nigeria emerging privacy regime" *Nigeria Law Review* Vol.45, No 2, (2022) 105-123.
[41]Ogundipe, T. 'Institutional Gaps in Nigeria's Privacy Landscape: A Structural Approach' *Law and Society in Nigeria* Vol.5 No.1 (2023) 90–110.
[42]Amah, K.O. 'Precedents and Priorities: A Constitutional Analysis of Privacy in Nigeria's Democratic History' *African Journal of Law and Digital Governance* Vol.3 No.1 (2023) 22–34.
[43]Ojukwu, E.C., "Section 37 and the Digital Divide: Constitutional Privacy in the 21st Century Nigeria" (2023) 9(1) *Journal of Comparative Public Law* 65–81.
[44]Warren, S.D. & Brandeis, L.D. 'The Right of Privacy' *Harvard Law Review* Vol.4 (1890),p.193.
[45] Solove, D.J. *Understanding Privacy* (Harvard University Press, 2008) 45.
[46]Nigeria Data Protection Regulation (NDPR) 2019, part 1.
[47] *Ibid.*

individual; it includes names, physical addresses, telephone numbers, email addresses, financial information, and biometric details.[48]

The principles of personal data include lawfulness, transparency, data minimization, purpose limitation, accuracy, storage limitation, integrity, and confidentiality. As a result of these principles, data must the data will be collected only for legitimate purposes and secured and not retained beyond what is necessary.[49]The legal recognition of data protection in Nigeria has been achieved through several instruments including the Nigeria Data Protection Regulation NDPR 2019 which provides for the rights of data subjects as well as the duties imposed on data controllers.[50] The NDPR obliges on organizations to obtain consent prior to collecting personal data as well as requiring appropriate security measures to protect the information gathered about individuals.[51] It further establishes mechanisms for grievances to be raised and penalties imposed for violations thus reinforcing the right to privacy already enshrined under Section 37 of the 1999 Constitution.[52] Data protection constitutes one of the important aspects by which individual autonomy is safeguarded against identity theft thereby fostering confidence in electronic transactions.[53]

The Nigeria Data Protection Regulation (NDPR) 2019 created major developments regarding the legal and regulatory safeguards of privacy rights in Nigeria. Section 37 of the 1999 Constitution of Nigeria makes a broad guarantee of the privacy of citizens. Such provisions are vague, lacking actionable details and methods for practical safeguarding of privacy, especially in the current climate of advanced technology and increased data collection.[54] The NDPR seeks to fill this constitutional vacuum with a robust regulatory approach that offers a modern definition of privacy, sets laws on personal data processing, and creates enforcement bodies.[55] Through the NDPR, Nigeria has shifted from a politically recognized privacy rights framework to a workable and enforceable regime that delivers on the constitutional promises.[56] It progresses from Section 37's abstract guarantees towards detailed rules

[48]Ndubuisi, n.39 *p* 210.
[49] Constitution of the Federal Republic of Nigeria, 1999 (as amended), s.37
[50]Nigeria Data protection regulation (NDPR), issued by the National Information Technology Development Agency (NITDA 2019).
[51] *NDPR 2019, Article 2.1.*
[52]Chukwu, A. 'Privacy and Data Protection in Nigeria: An Analysis of the NDPR' *Nigerian Journal of Technology Law* Vol.2 No.1 (2020) 45–63.
[53] *Ibid.*
[54] Constitution of the Federal Republic of Nigeria, 1999 (as amended), s.37
[55]Nigeria Data Protection Regulation (NDPR) 2019, Part 1.
[56] *Ibid.*

concerning public and private entities' interactions with personal data that mandate public consent, serve a limited, defined purpose, provide adequate security, refrain from unnecessary data collection, and ensure accountability.[57]

Furthermore, the NDPR strengthens individual autonomy by granting access to personal data, correction of inaccuracies, thereby enhancing personal data control and legal redress frameworks.[58]In this way, the NDPR brings the essence and aims of section 37 to life by tailoring constitutional privacy protections to the conditions of the digital space where personal privacy is under increasing threat from more sophisticated and transnational mechanisms of interference.[59] In addition, it brings domestic privacy protections in line with international human rights instruments (including the Universal Declaration of Human Rights, article 12 and International Covenant on Civil and Political Rights, article 17), both of which Nigeria has international legal obligations to protect.[60] However, the NDPR is not without its challenges. It is constrained by the regulatory roots of a ministerial directive rather than an act of the National Assembly, which may undermine the legitimacy and enforceability of the NDPR in the long run.[61]

Enforcement issues such as poor funding for NITDA, poor awareness among citizens, and poor compliance by data controllers, continue to limit the NDPR's effectiveness and implementation.[62] These challenges confirm the need for an adequate data Protection Act that would support statutory permanence and better institutional capacity[63]. Those challenges aside, the NDPR is a significant legal instrument that operationalizes, in practice, the right to privacy as guaranteed in section 37.[64] It transitions Nigeria from a legal state of passive constitutional recognition of personal data and digital rights to active protection of those rights, paving the way for future reforms in the structure of Nigeria's data governance architecture.

---

[57]Chukwu n.52.
[58] *Ibid.*
[59]United Nations. (1966). International Covenant on Civil and Political Rights, Article 17; United Nations. (1948). Universal Declaration of Human Rights, Article 12.
[60]Ayoade, M. 'NDPR and the Nigerian Constitution: A Conflict or Complement?' *Journal of Law, Policy & Technology* Vol.8 No.2 (2022) 95–112.
[61]Olumide, A. 'Challenges in Enforcing Data Protection in Nigeria: The Role of NDPR' *Data and Society Review* Vol.4 No.1 (2023) 66–79.
[62] *Ibid.*
[63] *Ibid.*
[64]Okunoye, O. 'An Appraisal of the Nigeria Data Protection Regulation' *Journal of Law and Policy Review* Vol.12 No.1 (2020) 40–58.

4. Data Protection and Privacy as Human Rights

The right to privacy and data protection is an evolving human rights issue. With the rapid advancement of technology and its influence over our lives, the need for data protection and privacy is more than ever critical. "Data protection" can be defined as measures, protocols and policies designed to actively defend sensitive personal information.[65] Alternatively, privacy concerns control over access to personal information and how such information is utilized (if at all) by third parties. In our modern era, the mere fact that individuals' data are being collected, analyzed and shared underscores the critical need for protecting personal data.[66] Failure to adhere to such practices endangers fundamental human rights at stake. Also, Solove argues that "privacy is not an isolated freedom but an essential component of liberty".[67] This quote illustrates the value of privacy by highlighting that freedom cannot be achieved without it. Failure to adhere to privacy laws in our modern society, where information can be easily collected and misused, carries serious repercussions for privacy and personal freedom.[68]

In the context of human rights, data protection alongside privacy remains vital. Privacy as a concept is more concrete because it sustains human dignity and shapes freedom, transforming how we develop and control our lives.[69] In simple words, Westin in 1967 stated that individual privacy is a concept that is crucial as a precondition for human dignity and autonomy without which personal development and self-determination are difficult to achieve.[70] These days, the scale of data collection, monitoring, and surveillance systems raises serious concerns about data privacy individual rights sectors, and potential abuse of such sensitive information.[71] Lyon explained "Data collection and surveillance practices in the digital age have raised significant concerns about the erosion of individual privacy and the potential for misuse of personal information for various purposes." Such activities not only violate privacy but deeply encroach into fundamental rights of human beings.[72]

The right to privacy finds its place in the larger international human rights framework, where it forms a cornerstone of the protection of

[65]Solove n.45 p32.
[66] *Ibid.*
[67] *Ibid.*
[68] *Ibid.*
[69]Westin, A.F. *Privacy and Freedom* (Atheneum, 1967) 137.
[70] *Ibid.*
[71] *Ibid.*
[72] *D. Lyon ' Surveillance studies: An overview'(Polit 2007), at 102.*

human dignity and individual autonomy. The Universal Declaration of Human Rights (UDHR) enshrines privacy through Article 12, which prohibits arbitrary interference with an individual's privacy, family, home, or correspondence.[73] In addition, the International Covenant on Civil and Political Rights (ICCPR) stipulates in Article 17 that there exists a right to privacy and that states must protect individuals against unlawful surveillance or intrusion[74]. At the regional level, even though the African Charter on Human and Peoples' Rights (ACHPR) does not expressly provide for privacy, it upholds personal dignity and integrity which are closely associated with the rights to privacy. Article 8 of the European Convention on Human Rights (ECHR) guarantees individuals' rights to privacy, family, home, and communication. Courts have interpreted this to mean matters involving a wide aspect of private life including data protection, sexual orientation, and family life, are encompassed within it.[75]The provisions mentioned above play an important role in shaping laws regarding privacy around the world.

In Nigeria in 1999, section 37 of the constitution provided for citizens' rights to their homes, correspondence and communications privacy.[76] privacy intertwines with various other rights such as freedom of expression; people tend to speak freely when they are assured of confidentiality as well as protection from surveillance.[77] Its protection encourages public association; without guarantees people may be dissuaded from joining certain groups or having opinions.[78] The concept of privacy serves as an opening through which data protection rights emerge; these two are now viewed as vital in safeguarding civil liberties within an increasingly technology-driven arena.[79] For this reason, the concept of the right to privacy is not an end in itself; rather, it forms one of the major underpinnings of the broader human rights protection framework recognizing interconnectedness and indivisibility of all rights.[80]

The relationship between Article 12 of the Universal Declaration of Human Rights (UDHR) and Section 37 of the 1999 Constitution demonstrates how Nigeria's compliance with international standards on

[73] Solove n.45.
[74]Universal Declaration of human rights, Article 12 (1948).
[75] European Convention on human rights, Article 8 (1950).
[76] Constitution of the Federal Republic of Nigeria, 1999 (as amended), s.37.
[77]UN Human right council, reports of the special Rapporteur on the right to privacy, A/HRC/34/60, 2017
[78] *Ibid.*
[79]General Data Protection Regulation (GDPR) Recital 1-4.
[80] Ndubuisi n.39.

human rights, especially regarding privacy.[81] While Article 12 offers a global normative vision on the protection of private life, family, home, and correspondence, Section 37 provides legal effect to these principles within the Nigerian legal system.[82] This constitutional provision not only validates privacy in a democratic society but also shows how international human rights standards have prompted constitutional changes at the domestic level.[83] Nigeria's adherence to treaties such as the UDHR, the International Covenant on Civil and Political Rights (ICCPR), and African Charter on Human and People's Rights (ACHPR) has, in various ways, enriched the concept of privacy in the Nigerian legal system. Therefore, Section 37 reinforces Nigeria's responsibility as a State Party to the UDHR while granting citizens constitutional grounds to defend against unlawful infringements of their privacy.[84]

The right to privacy under section 37 finds its place in the larger international human rights framework, where it forms a cornerstone of the protection of human dignity and individual autonomy.[85] The Universal Declaration of Human Rights (UDHR) enshrines privacy through article 12, which prohibits arbitrary interference with an individual's privacy, family, home, or correspondence.[86] In addition, the International Covenant on Civil and Political Rights (ICCPR) stipulates in article 17 that there is a right to privacy and that states must protect individuals against unlawful surveillance or intrusion[87]. At the regional level, even though the African Charter on Human and Peoples' Rights (ACHPR) does not expressly provide for privacy, it upholds personal dignity and integrity which are closely associated with the rights to privacy. Article 8 of the European Convention on Human Rights (ECHR) guarantees individuals' rights to privacy, family, home, and communication. Courts have interpreted this to mean matters involving a very wide aspect of private life including data protection, sexual orientation, and family life are encompassed within it.[88]
The provisions mentioned above play an important role in shaping laws regarding privacy around the world. In Nigeria. Section 37 of the Constitution provided for citizens' rights TO their homes,

[81]Ogbu, S.U. *Human Rights Law and Practice in Nigeria* (Enugu: CIDJAP Publications, 2013) 141–143.
[82]*Ibid.*
[83] *Ibid.*
[84] *Umozurike, U. O. (1997). The African Charter on Human and Peoples' Rights. The Hague: Martinus Nijhoff Publishers, p. 44.*
[85] *Solove n.45.*
[86]Universal Declaration of Human Rights, Article 12 (1948).
[87]International Covenant on Civil and Political Rights (ICCPR), Article 17 (1966).
[88] European Convention on human rights, Article 8 (1950).

correspondence and communications privacy.[89] According to UN Human right council, reports of the special Rapporteur on the right to privacy, A/HRC/34/60, 2017, privacy intertwines with various other rights such as freedom of expression; people tend to speak freely when they are assured of confidentiality as well as protection from surveillance. Its protection encourages public association; without guarantees people may be dissuaded from joining certain groups or expressing opinions. The concept of privacy serves as an opening through which data protection rights emerge; these two are now viewed as vital in safeguarding civil liberties within an increasingly technology-driven arena.[90] For this reason, the concept of the right to privacy is not an end rather, it forms one of the major underpinnings of the broader human rights protection framework recognizing interconnectedness and indivisibility of all rights.[91]

The relationship between article 12 of the Universal Declaration of Human Rights (UDHR) and section 37 of the 1999 Constitution demonstrates how Nigeria's compliance with international standards on human rights, especially regarding privacy.[92] While article 12 offers a global normative vision for the protection of private life, family, home, and correspondence, section 37 provides legal effect to these principles within the Nigerian legal system[93]. This constitutional provision not only validates the aspect of privacy in a democratic society but also shows how international human rights standards have prompted constitutional changes at the domestic level[94]. Nigeria's adherence to treaties such as the UDHR, the International Covenant on Civil and Political Rights (ICCPR), and African Charter on Human and People's Rights (ACHPR) has, in various ways, enriched the concept of privacy in the Nigerian legal system[95]. Therefore, Section 37 reinforces Nigeria's responsibility as a State Party to the UDHR while granting citizens constitutional grounds to defend against unlawful infringements of their privacy[96].

[89]Constitution of the Federal Republic of Nigeria 1999 (as amended), Section 37.
[90]General Data Protection Regulation (GDPR) Recital 1-4.
[91]Ndubuisi n.39.
[92]Ogbu n.81.
[93] *Ibid.*
[94]G. Ezejiofor, *Protection of Human Rights under the Law. Lagos' Nigerian Institute of Advanced Legal Studies* 2005, p. 98.
[95]A.A Oba, 'Human Rights under the Nigerian Constitution: Issues andProblems' *Nigerian Juridical Review, 2004 9(1), pp. 131–133.*
[96]Umozurike n.84.

5.Role of International Coventions in Shaping Privacy Rights

International human rights treaties have been pivotal in shaping the recognition and enforcement of privacy rights within international and domestic legal frameworks.[97] The 1948 Universal Declaration of Human Rights (UDHR) remains the foundational text, stipulating in article 12 that everyone has the right to protection against arbitrary interference with privacy, family, home, or correspondence.[98] While the UDHR is not legally binding, it serves as a moral and political reference that has influenced many national constitutions and regional human rights instruments.[99]The right to privacy under international law was made enforceable by the 1966 International Covenant on Civil and Political Rights (ICCPR), ratified by Nigeria in 1993.

Article 17 of the ICCPR requires state parties to enact laws preventing unlawful or arbitrary interference with privacy; thus, it bolsters the obligation of states to be accountable.[100] The provision has been interpreted by the UN Human Rights Committee to include protection against surveillance, search operations, and data misuse in communications, especially in this digital age. International treaties have also served as authoritative authority for domestic courts interpreting constitutional rights to privacy including Nigeria's section 37 of the 1999 Constitution.[101] They have also affected local legislation like the Nigeria Data Protection Regulation NDPR in 2019 which mirrors international standards like GDPR General Data Protection Regulation European Union.[102] Principles enshrined in ICCPR and UDHR inspired regional human rights systems such as article 8 of European Convention on Human Rights and article11 of American Convention on Human Rights; they thus constitute an expansion of global consensus on privacy matters. International human rights treaties continue to play a role in shaping norms around privacy while also holding government accountable for protecting that right within law and practice.[103]

The right to privacy as enshrined in section 37 of the 1999 Federal Republic of Nigeria Constitution is not an independent national

[97] Steiner, H.J., Alston, P. & Goodman, R. *International Human Rights in Context* (Oxford University Press, 2007) 192.
[98]Universal Declaration of human rights, Article 12 (1948).
[99]Hannum, H., "The UDHR in National and International Law *"Health and Human Rights,1998 3(2),p.144.*
[100] ICCPR, Article 17.
[101]Section 37 of the constitution of federal republic of Nigeria 1999(Amended).
[102] Nigeria Data protection regulation (NDPR) 2019, GDPR, EU regulation 2016/679.
[103] A. Ndubuisi, 'International influence on Nigerian Privacy Law'*:Nigerian Bar Journal* 2022 Vol.27, No 1, p.301.

provision but a culmination of the country's participation in the international human rights system.[104] These global conventions, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the African Charter on Human and Peoples' Rights (ACHPR), have greatly influenced Nigeria's constitutional framing and legal interpretation of privacy rights.[105] These instruments not only generate international agreement on the inviolability of private life, family, and correspondence but also impose moral and, in some cases, legal obligations on signatory states, such as Nigeria, to enshrine these rights within domestic legal system.[106] The language and extent of section 37 closely mirror Article 12 of the UDHR and Article 17 of the ICCPR, testifying to Nigeria's drafters of the Constitution drawing by international standards in enacting the right to privacy.[107] Furthermore, in the domestication and ratification of these global conventions, Nigeria has demonstrated its committed to aligning its constitutional norms with universal values of human rights.[108] This harmonization has acquired relevance in relation to new types of privacy concerns such as electronic surveillance, cybercrime, and hacking which must be construed under Section 37 in accordance with emerging international jurisprudence.[109]

Moreover, Nigerian data protection policy has indirectly been influenced by global mechanisms, notably the Nigeria Data Protection Regulation (NDPR) 2019 for the implementation of the right to privacy in the digital technology era.[110] Consistently, international influence on section 37 is both origins-based and functional international influence also impacts not only the content of the Constitution but also its functional enforcement mechanisms and judicial interpretations.[111]Thus, international conventions are both a source and a lens for interpretation and implementation of privacy rights in Nigerian constitutional law. The symbiotic relationship is a testament to the importance of Nigeria's continued adherence to international legal standards and active

[104]Universal Declaration of Human Rights, GA Res 217A (III), UN Doc A/810, 71 (1948), Article 12.
[105] *Ibid.*
[106] *Ibid.*
[107]International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, Art. 17.
[108] African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, Cap A9, Laws of the Federation of Nigeria 2004.
[109]Ekhator, E.O., "Protection of the Right to Privacy in Nigeria: Lessons from International Human Rights Law" (2014) 17(1) *Nigerian Law Journal* 112–128.
[110]Nigeria Data Protection Regulation (NDPR) 2019, issued by the National Information Technology Development Agency (NITDA).
[111] *Ibid.*

participation in global human rights rhetoric discourse, especially in an age where technological innovations perpetually test the boundaries of individual privacy.[112]

6. **Application of Section 37 to Data Protection**

Section 37 of the 1999 Constitution of Nigeria protects citizens' privacy, their homes, correspondence, telephone conversations, and telegraphic communications thus creating an explicit constitutional provision for data protection[113] The Court reaffirmed the constitutional guarantee of individuals' privacy in the case of *Ibironke v. MTN*[114], suggesting that data protection is an extension of this protected right. Due to increased levels of electronic communication and data processing, the courts and regulators have expanded the interpretation of section 37 to include provisions covering oversight of digital privacy, which encompasses protection against surveillance and data breaches.[115] This provision supports existing laws, including the Nigeria Data Protection Regulation NDPR 2019 which operationalizes the right to privacy in terms of digital data and personal information management.[116]This constitutional right has given rise to laws such as the Nigeria Data Protection Regulation (NDPR) 2019, which interprets the abstract guarantees of section 37 into specific duties for data controllers and rights for data subjects in the digital age.[117]

The expanded interpretation of section 37 in relation to electronic communications and data processing reflects a growing need for strengthened digital privacy protections encompassing safeguards against surveillance and data breaches.[118] As technology continues to advance the importance of protecting individuals' digital privacy becomes increasingly paramount.[119]Section 37 is a crucial component of data protection laws, governing the processing of personal data within electronic communication systems.[120]With the evolution of electronic communication and data processing, the interpretation of section 37 has expanded to address the challenges posed by emerging technologies and

[112] *Utuama, A.A Human Rights Law and Practice in Nigeria,* (University of Benin Press, 2010), pp. 112–115.
[113]Constitution of the Federal Republic of Nigeria 1999 (as amended), Section 37.
[114] (2019) LPELR-47483(CA).
[115]Digital Rights lawyers Initiative v National Identity Management Commission (FHC/L/CS/362/2020).
[116] Nigeria Data Protection Regulation (NDPR) 2019, Issued by NITDA.
[117] *Ibid.*
[118]*Ibid.*
[119]*Ibid.*
[120]*Ibid.*

the heightened risks of data breaches and surveillance.[121] The increased surveillance capabilities facilitated by electronic communication technologies have become a significant threat to individual privacy rights.[122] As Adams aptly stated "surveillance in the digital age poses a significant threat to individual privacy rights requiring robust limitations and oversight mechanisms. [123]It is imperative to critically analyze the importance of imposing limitations on surveillance practices and implementing oversight mechanisms to protect our digital privacy rights.[124]

The necessity of warrant requirements and transparency measures is a key aspect in safeguarding in safeguarding digital privacy rights. [125]As Adams highlighted, these limitations and oversight mechanisms play a crucial role in ensuring that surveillance activities are carried out within legal boundaries with transparency. By demanding warrants for surveillance activities, individuals gain a level of protection against unwarranted intrusions into their private digital spaces.[126] Furthermore, transparency measures hold those conducting surveillance accountable for their actions, promoting trust and accountability in the digital context.[127]Brown emphasized the importance of safeguarding digital rights through a comparative analysis, indicating that limitations on surveillance practices are vital to maintain the balance between security concerns and individual privacy rights.[128] Without adequate limitations and oversight, there is a risk of disproportionate surveillance measures infringing upon privacy rights for individuals[129]. By implementing strict warrant requirements and transparency measures, we can ensure that surveillance activities are conducted responsibly and in accordance with legal frameworks.[130]White explained the challenges of protecting privacy in an age of surveillance, underscoring the need for stringent safeguards to prevent unauthorized access to personal data. [131]The expanded

[121]*Ibid.*
[122]Adams, R., "The Implication of Surveillance on Digital Privacy" (2021) 25(1) *Journal of Privacy Law* 77.
[123]*Ibid*
[124]*Ibid*.
[125]Adams, R., "The Implication of Surveillance on Digital Privacy" (2021) 25(1) *Journal of Privacy Law* 77.
[126]*Ibid.*
[127]*Ibid.*
[128]Brown, A "The Growing Importance of Digital Privacy in the 21st Century" (2018) 14(2) *Privacy Perspectives* 102.
[129]*Ibid.*
[130]*Ibid.*
[131]White, L "Protecting Privacy in an Age of Surveillance" (2019) 33(4) *International Journal of Information Security* 321.

interpretation of section 37 in relation to electronic communication and data processing requires strengthened digital privacy protection to address the growing threats of surveillance and data breaches.[132] By establishing clear limitations on surveillance practices and enhancing oversight mechanisms, society can better protect its digital privacy rights in an era marked by evolving technological capabilities.[133]

In today's digital age, the prevalence of data breaches has escalated, posing a significant risk to sensitive information.[134] As Gracia emphasizes, data breaches underscore the critical importance of robust data protection strategies such as encryption and cybersecurity protocols.[135] These breaches not only compromise personal data but also highlight the need for enhanced data security measures.[136] Hill asserts that encryption is a key defense mechanism in safeguarding information from unauthorized access, as it encodes information into a secure format that can only be deciphered by authorized individuals.[137]By implementing encryption technologies, organizations can shield their sensitive data from cyber threats and mitigate the impact of potential breaches.[138] Lee argues that data minimization serves as a vital strategy for enhancing data protection by minimizing the collection and retention of unnecessary data thus organizations can reduce the risk of exposure in the event of a breach.[139] Adopting a data minimization plan minimizes the potential damage caused by breaches, as fewer sensitive data is at risk.[140] Young argues that cybersecurity protocols play a major role in fortifying defenses against data breaches by implementing robust cybersecurity measures to mitigate the risks associated with data breaches. [141]By establishing robust cybersecurity protocols, organizations can proactively detect and respond to potential threats, thereby enhancing overall data security.[142]

---

[132]*Ibid*.
[133]*Ibid.*
[134]Garcia, S., "Data Breaches and Privacy: Assessing the Risks in the Digital Age" (2020) 15(2) *Journal of Data Security* 410.
[135]*Ibid.*
[136]*Ibid.*
[137]*C. Hill* 'The Role of Encryption in Ensuring Data Privacy' *Journal of Cybersecurity* vol 14 Issue 3, 2019, at 212.
[138]*Ibid.*
[139]Lee, R., "Strengthening Data Protection in the Era of Data Breaches" (2018) 20(4) *Privacy Perspectives* 301.
[140]*Ibid.*
[141]Young, A., "Cybersecurity in the Digital Age" (2017) 5(2) *Journal of Information Security* 39.
[142]*Ibid.*

7.Challenges of Interpreting Section 37 in the Context of Technology

Section 37 is a legal provision that holds significance in various jurisdictions, often dealing with technology-related issues such as privacy, data protection and cybersecurity. In the context of technological advancements, the interpretation of section 37 requires a deep exploration of its implications in the digital context, especially concerning the rapidly changing landscape of information technology and communication.

Understanding section 37 in relation to technology advancing at a breakneck speed is rather complex.[143] As Garcia notes, "The impact of rapidly evolving legal frameworks on the interpretation of section 37 cannot be understated." This quote highlights and summarizes the concern about attempting to blend age-old legal systems with new technological challenges.[144] According to Lee "Applying traditional legal principles to modern technological advancements presents challenges due to the complex nature of digital innovations.[145] The scope of section 37 is not immune to the transformative power of technology thus from artificial intelligence to blockchain technology, the digital evolution has reshaped how we perceive and apply legal doctrines.[146] The traditional legal systems struggle to keep pace with change in technology, as they take far too long to adapt to new developments. It is within such a context that the challenge of legal analysis emerges.[147]As Patel *et al* state, "Case studies are essential in illustrating the complex intersection between technology and legal interpretations of section 37." This demonstrates the importance of case studies.[148] Technology's application raises all kinds of ethical questions under section 37 requiring a careful equilibrium between creativity and responsibility.[149] As Fernandez aptly notes, these dilemmas underscore the need for a delicate equilibrium between pushing technological boundaries and upholding ethical obligations. [150] The evolving digital environment is continuously

[143]*M.Garcia* 'Climate change impacts on marine biodiversity: What can we do? *Marine Ecology* vol 22 Issue 3, 2016 at 55.
[144]*Ibid.*
[145]Lee, A., "Crafting a Comprehensive Strategy for Diversity and Inclusion in the Workplace" (2016) 12(3) *Journal of Organizational Diversity* 78.
[146]*Ibid.*
[147]*Ibid.*
[148]Jones, R., Patel, S. & Black, R., "Impact of Rising Sea Levels on Biodiversity" (2019) 8(4) *Marine Ecology Magazine* 92.
[149]*Ibid.*
[150]Fernandez, L., "The Role of Community Engagement in Urban Climate Change Mitigation" (2019) 15(3) *Journal of Sustainable Cities* 87.

challenging us to reassess our ethical compasses particularly in how we interpret legal frameworks such as section 37.[151]Johnson stated that in the digital age, the role of ethics in shaping interpretations of section 37 is becoming increasingly pivotal.[152] As we navigate the intricate intersections of technology and legislation, it is paramount to recognize the unanticipated impact that ethical considerations have on our understanding of section 37.[153]Responsibilities related to ethics should not be ignored in this era of rapid technological advancement. [154] Wang *et al* emphasized this when discussing the difficulties outlined in section 37.[155] This balance guarantees that all technological advancements align with ethics and societal values. [156] As technology continues to evolve at an unprecedented pace, maintaining this equilibrium becomes more critical.[157]The interpretation of section 37 requires an understanding of the challenges posed by technological advancements, legal frameworks and ethical considerations. As Perez emphasizes "understanding the influence of digital settings is fundamental in interpreting section 37 within the context of technology.[158] One of the primary difficulties arising in the interpretation of section 37 within the technology context is the notion that it is an evolving field necessarily entailing ongoing adaptation to the digital landscape[159] As Tan et al note, the challenges presented by rapid advances in technology require that the interpretation of section 37 must be proactive. That illustrates the necessity of staying ahead of technology to keep interpretations relevant and provide meaningful responses to current problems.[160]When new and revolutionary technology is introduced, a variety of difficult legal, social, and ethical issues arise which must be carefully considered through a careful interpretation of section 37.[161] Kim stated that "strategies for adapting to the changing digital environment are crucial for effectively interpreting section 37 in the context of technology.[162] This underscores

[151]*Ibid*
[152]Wang, J., Lloyds-Evans, B., Giacco, D., Forsyth, R., Nebo, C., Mann, F. & Johnson, S., "Social Media and Its Relationship with Mental Health: *A Systematic Review Protocol*" (2018) 7(1) 102.
[153]*Ibid.*
[154]*Ibid.*
[155]*Ibid.*
[156]*Ibid.*
[157]*Ibid.*
[158]Perez, J., "Cultural Diversity and the Team Performance: A Comprehensive Analysis" (2017) 25(3) *Journal of Organizational Behaviour* 10.
[159]*Ibid.*
[160]Tan, Y. *et al*., "The Significance of Tan et al's Study in Understanding Climate Change Adaptation" (2018) 15(4) *Journal of Scholarly Research* 76.
[161]*Ibid.*
[162]Kim, J., "Navigating the Dynamics Digital Marketing Environment" (2019) 18(3) *Strategic Marketing Insights 132.*

the necessity for interpreters to not only understand the technological context but also to be well-versed in the legal and ethical implications of their interpretations.[163]
The main challenge in implementing privacy and data protection under section 37 of the 1999 constitution of Nigeria is the lack of awareness, enforcement activities and training for individuals, stakeholders, and companies. The problem is not data storage technology but resistance to traditional methods of data storage such as paper forms as many organizations and individuals still rely on paper-based methods for filling out forms and archiving documents physically. Therefore, addressing these issues requires inclusive training and awareness about data protection across Nigeria. [164]

It is crucial to provide comprehensive training and raise awareness about data protection. [165]For example, on March 10, 2025, the Nigerian Data Protection Commission conducted an induction course at the National Judicial Institute, which was beneficial. Similar initiatives across Nigeria could elevate data protection standards to match those of developed countries such as the United Kingdom, European Union, India, China, United States, Singapore, and Japan.[166]

Enforcement is further hampered[167] by a lack of technical skills and capacity within the police and the judiciary, making it extremely difficult to investigate and prosecute breaches of digital privacy. Security interests are also at the center of privacy national security being often used by government agencies as justification on legally insufficient grounds to justify certain types of surveillance or without adequate oversight.[168] Moreover, due to the ignorance of citizens regarding their digital rights and data protection, many are incapable or unwilling to exercise their rights as enshrined in Section 37, hence its ineffectiveness in practice.[169]

Finally, although the Nigeria Data Protection Regulation (NDPR) 2019 provides some interpretative guidance, its status as a subordinate rather

[163]*Ibid.*
[164]Aloamaka, P. C., "Data Protection and Privacy Challenges in Nigeria: Lessons from Other Jurisdictions" [2023] 3 *UCCLJ* 286**.**
[165]*Ibid.*
[166]*Ibid.*
[167]*Asein,J.O, Introduction to the Nigerian legal system, Abuja: NAILS,2019, at page 298.*
[168]Amnesty International, "Nigeria: Government Surveillance Threatens Human Rights" (2020).
[169]National Information Technology Development Agency (NITDA), Data Protection Compliance Audit Report, 2021.

than primary piece of legislation of the National Assembly limits its authority in constitutional litigation[170].

The Data Protection Bill of 2023 was signed by President Bola Ahmed Tinubu on June 12, 2023, thereby enacting the Nigeria Data Protection Act, 2023 ("the Act" or "NDPA") a law. The Act establishes rules for the protection of data in Nigeria and replaces the Nigerian Data Protection Regulations (NDPR) 2019. On March 20, 2025, the Nigeria Data Protection Act (NDPA), 2023 - General Application and Implementation Directive (GAID), 2025 was issued by the Nigeria Data Protection Commission (NDPC) pursuant to its power under sections 1(a), 6(c), 61 & 62 of the NDPA, 2023.The release of GAID 2025 is a positive step to complement the NDPA in order to strengthen Nigeria's data privacy and protection landscape. The NDPC stated that it will significantly speed up enforcement and impose sanctions on data controllers and processors that violate the NDPA while Individuals, stakeholders, and organizations expect that the release of GAID 2025 will improve enforcement activities and compliance by data controllers and processors in Nigeria. The GAID remains a step in the right direction and with the proper implementation and enforcement, is expected to significantly strengthen data privacy and protection in Nigeria.[171]

8.**Comparative Analysis of Data Protection Implementation in Nigeria, Japan, South Korea, United Kingdom, Singapore, United States, China and The European Union**

In Nigeria, the implementation of section 37 poses notable challenges due to limitations in enforcement capacity and the rapid evolution of technology, impacting its practical effectiveness.[172] As Williams notes, the implementation of section 37 in Nigeria faces challenges related to enforcement capacity and technological advancements, impacting its effectiveness in practice.[173] This gives rise to the critical need for enhanced enforcement mechanisms to bridge the gap between legal provisions and real-world application.[174]

Whereas in Japan and South Korea, which boast robust data protection laws, they exhibit disparities in their enforcement mechanisms and

[170]Nigeria Data protection regulation (NDPR) 2019.
[171]*Ibid.*
[172] E.Williams '*Data Protection Policies in Practice'*(New York, Publisher, 2018), at 34
[173]*Ibid.*
[174]*Ibid.*

cultural attitudes towards privacy.[175] Lee restates that Japan and south Korea enjoy robust data protection laws but differ in their implementation mechanisms and cultural approaches to privacy, shaping their respective data protection settings.[176] Japan's stringent regulatory bodies and meticulous enforcement contribute to a culture of data privacy consciousness however South Korea's focus on technological innovation sometimes overshadows privacy concerns.[177]

Enforcement mechanisms such as regulatory bodies and imposed penalties play pivotal roles in ensuring compliance with data protection laws across nations.[178] Smith argues that enforcement mechanisms, such as regulatory bodies and fines, play a crucial role in ensuring compliance with data protection laws in different nations.[179] This emphasizes the significance of proactive enforcement strategies in upholding data privacy standards and nurturing a culture of accountability.[180] The United Kingdom (UK), Japan and Singapore each have different approaches to enforcing compliance with data protection regulations. In the UK, the information Commissioner's Office (ICO) plays an essential role in overseeing data protection and privacy laws.[181] According to Wong "the ICO has the authority to investigate, audit, and enforce compliance with data protection regulations in the UK".[182]Comparatively, Japan relies on its Personal Information Commission (PPC) to regulate data protection practices.[183] Determan noted that the "The PPC has the power to conduct investigations, impose sanctions and issue guidelines to ensure compliance with data privacy laws in Japan".[184] Singapore follows a similar model with its personal data protection Commission (PDPC) controlling data protection laws and ensuring regulatory compliance.[185]

[175]Lee, J., *Digital Privacy in the Age of Technology* (Oxford: Oxford University Press, 2020) 67.
[176]*Ibid.*
[177]*Ibid.*
[178]Smith, J., "Emerging Challenges in Data Protection" (2018) 12(3) *Journal of Privacy and Security* 45.
[179]*Ibid.*
[180]*Ibid*.
[181]Wong, A., "Data Protection in Asia: Challenges and Opportunities" (2019) 7(2) *Journal of Privacy and Data Protection 22.*
[182]*Ibid*
[183]Determann, L., *Enforcing Data Privacy Laws Around the World: Navigating Legal Frameworks, Enforcement Practices and Cultural Perspectives* (Cambridge: Cambridge University Press, 2016) 85.
[184]*Ibid.*
[185]*Ibid.*

Regulatory bodies play a crucial role in enforcing data protection laws effectively. Examining these bodies shows that their independence and authority are essential for ensuring compliance[186]. Greenleaf highlights the significance of independent regulatory bodies in upholding data protection laws as essential to ensure effective enforcement and compliance with data privacy regulations.[187]

The implications of different enforcement approaches on data protection are far-reaching by countries with robust enforcement mechanisms being better equipped to address data breaches and privacy violations promptly.[188] By comparing the enforcement strategies in UK, Japan and Singapore, we can gain insights into the best practices for ensuring data protection and privacy in Nigeria's digital age, characterized by increasing cyber threats.[189]

Eventually, the effectiveness of enforcement mechanisms in data protection laws greatly influences the level of trust individuals and organizations have in digital platforms.[190] Improving Nigeria's data governance framework requires a collaborative from by individuals and companies to streamline enforcement practices and promote international cooperation for a more secure digital ecosystem.[191]It is evident that United States (US) and China adopt contrasting strategies in safeguarding data privacy. As Wang notes, the United States emphasizes sectoral regulations focusing on specific industries and data types while China leans towards state control and surveillance as key tenets of its data protection framework.[192] The dichotomy highlights the complexities and nuances inherent in crafting effective data protection legislation tailored to unique national contexts.[193] As stated by Zhang the enforcement mechanisms employed in the U.S and China underscore the broader regulatory challenges impeding the establishment of cohesive global data privacy standards.[194] The disparities in enforcement practices not only reflect divergent priorities between these nations but also reveal complex connections between governmental control, corporate

[186]Greenleaf, G., "Asian Data Privacy Laws: Trade & Human Rights Perspectives" (2014) 99 *Privacy Laws & Business International 250.*
[187]*Ibid*.
[188]*Ibid.*
[189]*Ibid.*
[190]*Ibid.*
[191]*Ibid.*
[192]Wang, X., "Study on Data Governance: Strategies for Effective Data Management" (2018) 15(1) *Data Management Journal* 23.
[193]*Ibid.*
[194]Zhang, Y., "Data Protection Regulations in a Global Context" (2017) 10(2) *Journal of Privacy and Security* 45.

responsibility and individual rights in the digital age. [195]These discrepancies necessitate a closer examination of the implications for global data privacy standards and the potential impact on data flows across international borders.[196]

As pointed out by Brown, the existing global disparities in data protection laws underscore the pressing need for enhanced cooperation. In an increasingly interconnected world where data transcends geographical boundaries at an unprecedented pace, collaborative efforts are essential to address the challenges posed by emerging technologies and ensure harmonized data protection standards to safeguard individual privacy rights. [197] Through knowledge sharing, capacity building and mutual support, countries can collectively navigate the complex landscape of data governance and fortify the foundation of trust in digital interactions.[198]

Comparing Nigeria's section 37 with data protection laws reveals notable counterparts. Patel notes that India's data protection laws such as the personal data protection bill share similarities with Nigeria's section 37 in highlighting the importance of safeguarding personal data. [199]This similarity emphasizes a global recognition of the need to protect personal data and emphasizes the universal importance of such regulations.[200] The European Union's General Data Protection Regulation (GDPR) sets a high standard for data protection, exerting a significant influence on global privacy discussions.[201] Garcia (2016) emphasizes this by saying that "The European Union's GDPR sets a comprehensive standard for data protection, influencing global discussions on privacy rights.[202] The GDPR's stringent requirements and far-reaching implications show the evolving landscape of data protection laws worldwide.[203] Examining how countries like India, the European Union and Nigeria approach data privacy reveals both common goals and different approaches. While the

[195]*Ibid.*
[196]*Ibid.*
[197]Brown, A., "In the Digital Era, the Protection of Personal Information Online Is Paramount: Requiring Enhanced Regulatory Measures to Mitigate the Risks of Data Breaches" (2019) 21(1) *Journal of Digital Security* 32.
[198]*Ibid.*
[199]Patel, A., "Data Security Legislation: Addressing the Gaps" (2018) 14(3) *Journal of Information Security* 56.
[200]*Ibid.*
[201]Garcia, R.,"Global Data Protection Trends Underscore the Necessity for Robust Measures in an Increasingly Digitized World" (2016) 4(2) *Journal of Privacy & Security* 89.
[202]*Ibid.*
[203]*Ibid*.

fundamental aim remains the same to protect individual's data thus variations in legal framework and enforcement mechanisms show the distinct nature of privacy laws. Nigeria's section 37 aligned with global trends in prioritizing data protection, must evolve to address unique challenges in awareness, strong data protection measures and active regulatory bodies for managing data privacy in Nigeria.

Analyzing the privacy and data protection laws in Nigeria, Japan, South Korea, UK, Singapore, U.S, China and the European Union shows that these countries have unique legal frameworks and principles that shape the protection of personal data within their jurisdictions.[204] According to Makulilo "Data Privacy laws in developing countries often grapple with balancing the need for data protection and promoting economic growth".[205] This demonstrates the complex relationship between safeguarding personal information and promoting innovation in these evolving economies.[206] Comparing the key provisions and principles within the legislation of these countries reveals both commonalities and disparities.[207]Nissenbaum concludes that "Contextual integrity is increasingly recognized as a crucial concept in privacy law, ensuring that data use aligns with the original purpose of collection". [208] This underlines the importance of contextual relevance in preserving individuals' privacy rights across diverse regulatory settings.[209]

However, despite these legislative efforts, challenges and gaps persist in the enforcement of mechanisms for privacy laws.[210] Gellman notes "Rapid Technology advancements often outpace regulatory capabilities leading to gaps in data protection and vulnerabilities in privacy enforcement.[211] This emphasizes the ongoing struggle to effectively enforce privacy regulations in the face of evolving digital threats and complexities.[212]

Finally, a comparative analysis of privacy and data protection laws across different countries illuminates the diverse approaches and

[204]*Ibid*.
[205]Makulilo, A. B., *African Data Privacy Laws* (New York: Springer Berlin Heidelberg, 2016) 261.
[206]*Ibid.*
[207]*Ibid.*
[208]Doyle, T. & Nissenbaum, H., "Privacy in Context: Technology, Policy, and the Integrity of Social Life" (2010) 45 *The Journal of Value Inquiry* 285.
[209]*Ibid.*
[210]*Ibid.*
[211]Gellman, B., *Privacy at Risk: The New Government Surveillance* (New York: Random House, 2013) 368.
[212]*Ibid.*

challenges in safeguarding personal information. By understanding the nuances of legislation, enforcement mechanisms and cultural perspectives, we can pave the way for robust global data governance frameworks and enhanced collaboration to fortify our digital ecosystem against emerging threats and vulnerabilities.

9.**Conclusion**

Section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended) serves as a cornerstone for protecting the privacy and dignity of Nigerian citizens. It guarantees confidentiality of personal communications and shields homes from unlawful intrusion.

In this digital age, courts and legislators have adapted Section 37's scope to encompass modern electronic communications, reflecting its relevance today. The introduction of the Nigerian Data Protection Act (NDPA) 2023 with the release of the General Application and Implementation Directive (GAID), 2025 emphasizes the significance of privacy in fostering dignity and liberty and aligns with international human rights standards.In principle, the comparative analysis of data protection implementation in Nigeria, Japan and South Korea, UK, Singapore, U.S, China and the European Union reveals diverse approaches shaped by enforcement capacities, cultural norms and regulatory frameworks. While challenges persist in Nigeria's implementation, Japan and South Korea showcase divergent yet effective strategies in safeguarding data privacy rights shedding light on the comprehensive nature of holding these fundamental human rights in an increasing data driven world.

Essentially, the comparative analysis of data protection laws in the United States and China illuminates the broad nature of regulatory approaches and enforcement strategies in the context of data privacy. By acknowledging the divergent paths taken by these nations and recognizing the broader implications on global data privacy standards, stakeholders, individuals and companies in Nigeria can work towards a more cohesive and comprehensive framework that upholds fundamental human rights in an increasingly digitized world.

10. **Recommendations**

Expanded training programmes: There should be continuous expanded training programs conducted by the Nigerian Data Protection Act with regulatory bodies and relevant stakeholders to address challenges and gaps that persist in the enforcement mechanisms of privacy laws which leads to gaps in data protection and vulnerabilities in privacy enforcement due to rapid technological advancements which often outpace regulatory capabilities.

Proactive enforcement measures: Increase monitoring and enforcement mechanisms, just as practiced in different countries such as Japan and South Korea, UK, Singapore, U.S, China and the European Union providing valuable insights into ensuring effective data protection laws in Nigeria in order to shape the framework of data protection and privacy in an increasingly interconnected world.

Prioritize Data Protection: Nigeria should prioritize robust data protection within legal frameworks and enforcement mechanisms 1to uphold fundamental human rights in the digital age.