NAVIGATING THE TENSIONS BETWEEN DATA PRIVACY AND NATIONAL SECURITY: A COMPARATIVE ANALYSIS OF NIGERIAN AND INTERNATIONAL LEGAL FRAMEWORKS

OKOHO, Etim[1]

Abstract

The interaction between data privacy and national security is positioned by modern research as one of the urgent legal and policy questions of international concern. Swift technological advancement and a growing security threat have been the characteristics of Nigeria, which has seen a corresponding expansion of state surveillance capabilities, a trend that often serves to compromise the privacy interests of individuals. The current paper analyses the conflict between the right to privacy of personal information and national security in the Nigerian legal system. The main aims of it are to question the sufficiency of the data-protection and national-security systems in Nigeria, to identify the sources of conflict and suggest the balanced solutions that do not undermine the civil liberties but support the effective security measures. The study is methodologically grounded within the doctrinal research methodology. Comparative analysis compares the approach of Nigeria to that of the European Union, the United States and the United Kingdom thus providing insight on how these jurisdictions treat privacy security dilemma. The results reveal that the data-protection system in Nigeria can be described as underdeveloped, where there is poor monitoring of the system and a wide range of discretionary powers granted to security agencies with limited accountability. To this end, the research suggests building on the legal protection, enhancing institutional protection, and embracing global good practices to create a more coherent and rights-respecting balance between privacy and security of data and national security.

Key Words: Data Privacy, National Security, Surveillance Law, Cybersecurity, Digital Rights

1. Introduction

The development of digital technology and the increasing dependence on data-based systems have contributed to the scholarly and practical discussions of the issues of data privacy and governmental surveillance. Electronic surveillance is also being used by governments, often with insufficient legal check and balances, to track and collect personal information in the name of national security. This tension between the protection of privacy and national security is particularly intense in developing democracies like Nigeria, where the legal and institutional protection is still in its infancy. Although Nigeria's 1999 Constitution affirms the right to privacy under Section 37, statutes including the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and the Terrorism (Prevention) Act 2011 (as amended) confer expansive powers on security and intelligence agencies for data collection and surveillance activities. These provisions are often lacking in explicit checks and balances, thereby inviting scrutiny over potential abuse and the attenuation of civil liberties.[2]

Cross-jurisdiction comparative analysis reveals that other jurisdictions have similar tensions. In the European Union, the General Data Protection Regulation (GDPR) establishes robust protection rights while allowing limited derogations for national security, provided such measures are demonstrably necessary and proportionate.[3] In the United States, controversies surrounding the USA PATRIOT Act and various mass surveillance programmes exemplify the delicate equilibrium required in liberal democracies between

[1] **OKOHO, Etim, LLB, BL, LLM, PhD (in view),** (Chief Legal Officer, Directorate for Establishment of Private Universities, National Universities Commission, Abuja & PhD Candidate Nasarawa State University Keffi) okohoetim85@gmail.com, oeetim@nuc.edu.ng - 26, Aguiyi Ironsi Street, Maitama, Abuja; 08030844330.

[2] O. Olatunji, "Surveillance and the Right to Privacy in Nigeria: A Legal Analysis" *Nigerian Journal of Cyber Law and Data Protection* [2022] (1) (2) 33.

[3] B. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) 95.

security and privacy.[4] Together, these experiences provide light into what is possible to design in terms of legal frameworks that can respect individual rights but still maintain state security interests. This paper carries out a critical evaluation of the legal system of Nigeria in balancing the protection of data privacy and the national security concerns. It mainly aims to evaluate the compatibility between the data-protection regime of the country and the national-security laws and to evaluate whether this regime provides sufficient protection of fundamental rights. The analysis also addresses the question of whether lessons learned in other jurisdictions as well as comparative jurisdictions (the European Union, the United States, and the United Kingdom) can be applied to possible legal and policy changes. The study will be doctrinal in approach and will focus on the analytical examination of statutes, constitutional provisions and case laws. An international approach is presented, which uses the experiences and law of the jurisdictions identified.

The research is limited to the legal and institutional frameworks that regulate the access of the state to personal data in Nigeria. It covers the normative basis of data privacy, the extent of limitations that can be made in the name of security and the control structures that are required to make it accountable. It is not directly evaluated in technological and operational terms; instead, the discussion is concerned with the normative legal issues that are presented by the existing framework. Through this, the paper contributes to the current debate on the legal reforms that are needed to have a balanced and rights-respecting data-governance regime in Nigeria.

2. Conceptual Framework

2.1 Defining Data Privacy and National Security

Data privacy is a legal and ethical obligation that requires personal data to be safeguarded against unauthorised access, use or disclosure. It encompasses the right of an individual to control the gathering, processing, and sharing of information, particularly in the digital space. Contemporary discussions of data privacy rest on the principle of informational self-determination, which affords individuals the autonomy to decide how their data are handled.[5] The emergence of this principle is a result of the exponential growth of digital communications, surveillance technologies and data-driven decision-making systems.

National security on the other hand involves safeguarding the sovereignty, territorial integrity, safety of people and the institutions of a nation against both internal and external attacks. These threats can be in the form of terrorism, cyberattacks, espionage, subversion, etc. In the post-9/11 era, national security has broadened to encompass digital and informational vulnerabilities as well as traditional physical threats.[6] Governments therefore assert their rights to gather and interpret information including personal communications, in the name of intelligence-gathering and pre-emptive security. Despite the fact that data privacy and national security are both invaluable in their own contexts, they often clash in real life, especially when the laws attempt to establish the degree to which the privacy of an individual can be invaded under the pretext of citizen security.

2.2 The Privacy–Security Dichotomy

The dialectic between privacy and security is no abstract theory; instead, it carries some practical implications on modern legal regimes, especially those that are weak in the rule of law protection. Even though privacy is a basic human right, it is not absolute and can be legally limited to serve some other good purpose like maintenance of national security or maintenance of public order. Any such limitation, however, must satisfy the criteria of legality, necessity, and proportionality.[7] In practice, governments tend to expand

[4] L. Donohue, "Bulk Metadata Collection: Statutory and Constitutional Considerations" *Harvard Journal of Law & Public Policy* [2015] (38) 13.
[5] D. J. Solove, *Understanding Privacy* (Harvard University Press, 2008) 24.
[6] L. Zedner, "Securing Liberty in the Face of Terror: Reflections from Criminal Justice" *Journal of Law and Society* [2005] (32) (4) 507.
[7] C. Kuner, "Balancing Privacy and National Security" *International Data Privacy Law* [2015] (5) (4) 225.

their surveillance abilities with minimal or no oversight and in most cases, they use the national security as a pretext to compromise privacy rights. Such a dynamic cultivates a "security exception culture" characterized by wide, discretionary authorities exercised in the absence of clear legal boundaries or rigorous judicial review.[8] As an example, data-interception laws can authorise mass surveillance without prior judicial approval or independent check, which jeopardises the creation of a surveillance state, particularly in situations where civil society and institutions are not capable of protecting privacy rights.

Comparative analysis brings out the existence of various regulatory routes. In the European Union, privacy is defined as a constitutional right in the Charter of Fundamental Rights and any restriction must be necessary. The United States, in contrast, adopts a more security-centric approach, allowing privacy protections to be superseded by statutory instruments such as the Foreign Intelligence Surveillance Act (FISA), subject to limited judicial scrutiny. The legal system of Nigeria is also based on recognizing privacy rights in the Constitution, but it still is oriented in favour of the state security interests, and it does not provide enough means of balancing these concerns. The main policy issue therefore is to develop legal regimes that respect the spirit of privacy but at the same time give the state the power to ensure that the nation is secure. This is a balance required to sustain the rule of law and the democratic values.

3. Legal Framework on Data Privacy and Surveillance in Nigeria

The data-protection system in Nigeria is still at an early stage, and it is dynamic, changing according to the rising number of cases related to privacy issues caused by the rise of digital surveillance. In spite of the fact that the Constitution has a constitutional right to privacy, a panoply of statutory and regulatory tools is deployed to give effect to that promise. However, there still exist inconsistencies between statutory and regulatory arrangements, the duplication of mandates, and poor enforcement frameworks, which in turn hinder the achievement of effective data governance in the nation.

3.1 Overview of Relevant Legislation

3.1.1 Constitution of the Federal Republic of Nigeria 1999 (as amended). Section 37

The Constitution of the Federal Republic of Nigeria 1999 (as amended) continues to serve as the country's supreme legal document, and Section 37 establishes the constitutional framework for the protection of privacy. The article states, "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and secured."[9]

By stating that the modern protections should also apply to the modern means of communication, such as e-mail, text messages, and online platforms, this clause gives data privacy a constitutional status in Nigeria. However, the text is vague in a number of ways: it fails to define digital data or biometric information and does not specify any acceptable limits to state intrusion. Furthermore, Section 45 authorizes derogations from fundamental rights in the name of public safety, order, defence, and morality, a broad mandate that has often been construed by courts as permitting surveillance activities under national security grounds.[10]

Judicial enforcement is the only form of enforcement with respect to Section 37.[11] In Nigeria, the courts are yet to establish a comprehensive jurisprudence on digital privacy and although the section provides a legal framework, it still needs supporting legislation and institutional frameworks to transform its guarantees into practical privacy rights.

[8] C. C. Murphy, "Surveillance and the Rule of Law: A Report on the UK Investigatory Powers Act 2016" *Cambridge Law Journal* [2017] (76) (2) 372.
[9] CFRN 1999. s 37
[10] O. Ojo, "The Constitutional Right to Privacy and Surveillance Practices in Nigeria" *Nigerian Journal of Human Rights Law* [2021] (3) (1) 44.
[11] CFRN 1999. s 37

3.1.2 Nigeria Data Protection Act 2023

The Nigeria Data Protection Act (NDPA) 2023 constitutes the most comprehensive legislative framework dedicated to the protection of personal data within Nigeria. Replacing the earlier Nigeria Data Protection Regulation (NDPR) 2019, the Act broadly defines personal data and articulates the principles of lawful processing, notably consent, purpose limitation, data minimisation, and transparency. In particular, the NDPA 2023 establishes the Nigeria Data Protection Commission (NDPC) as the principal regulatory authority for data protection. The Commission has the mandate to ensure compliance, audits, sanctions, and codes of conduct are in place and is empowered to carry out its work in both the public and the private sector processing the personal data of Nigerian residents and also those outside the country where the data is on residents of Nigeria.

The Act however has a wide range of exemptions, such as those under Section 30, which permits processing without the consent where it is required by national security, and in the interests of the nation, and any legal requirements. These exemptions are not narrowly defined, and the absence of robust judicial oversight mechanisms raises concerns about potential abuse.[12] Also, the Act lacks articulation of thresholds on access to data by security agencies, which can be interpreted and used by the executive in an overbearing manner.

3.1.3 Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 constitutes Nigeria's inaugural dedicated cybersecurity legislation. The statute brings a wide range of cyber-malicious acts under one umbrella by criminalising cyberstalking, hacking, identity theft, and online fraud. Most prominently, it grants the state authorities the power to intercept communications and access stored electronic data on a large scale. Section 38 gives the law-enforcement agencies the authority to intercept, record and monitor electronic communications in cases where it is deemed necessary during criminal investigations or national security. This allows the real-time access to traffic information and requires the service providers to provide such access to the state. However, no prior judicial authorisation is mandated, and the absence of an independent oversight mechanism renders this power susceptible to misuse.[13] Even though the Act was developed to enhance cyber-crime enforcement, its surveillance measures are not counter-balanced with equivalent safeguards in the form of necessity and proportionality requirements or an independent review process. As a result, the privacy that is guaranteed by the constitution is violated and an atmosphere of unregulated surveillance is created.

3.2 Institutional Framework (e.g., NDPB, NCC, etc.)

The institutional structure in Nigeria that deals with data privacy and surveillance is dispersed among various regulatory and enforcement agencies that have overlapping mandates to some extent. Central agencies include the Nigeria Data Protection Commission (NDPC), the Nigerian Communications Commission (NCC), and assorted law enforcement and intelligence agencies. The NDPC is the main regulator of data protection in Nigeria, which was established under the NDPA 2023. The Commission has the mandate of licensing data controllers and processors, investigating breaches of data, issuing compliance guidelines, and enforcing data subject rights. It is also mandated with the creation of sector-specific codes of practice and building awareness of the people on the principles of data protection.

The NCC as the regulator of telecoms also plays a central role since it monitors the telecommunications operators which should respond to the request of data by the security agencies. It presides over data retention, SIM card registration and interception regimes. However, due to its central mandate of service regulation

[12] F. Okoye, "Navigating Nigeria's Data Protection Act 2023: Rights, Obligations and Exemptions" *African Journal of Cyber Law and Digital Rights* [2024] (2) (1) 17.

[13] A. Adeoye, "A Legal Review of Interception Powers under Nigeria's Cybercrimes Act" *Journal of Law, Technology and Society* [2022] (4) (2) 63.

and technical compliance, the ability of NCC to protect the rights to privacy is limited.[14] Complementing these authorities are several security and intelligence agencies, the Department of State Services (DSS), National Intelligence Agency (NIA), and Nigerian Police Force (NPF), that wield surveillance powers in the name of national security. These agencies are operating in large part under shrouded mandates, and under limited parliamentary or judicial oversight, and do not have in place the comprehensive accountability mechanisms that would provide assurance of adherence to constitutional and statutory standards of privacy protection. The consequence is a fragmented and, at times, inefficient data governance regime, which is the legacy of the endemic malfunctions of coordination among these institutions, as well as the overlap of jurisdictions and regulatory gaps. Without a centralized control, the data rights of the individuals are at risk especially when faced with blanket surveillance by the state in the name of security.

4. National Security and State Surveillance Powers

Nigeria is faced with increased internal security threats such as terrorism, banditry, cybercrime, separatist agitations and violent extremism. The state has consequently made significant strides in beefing up its surveillance and intelligence-gathering abilities as a countermeasure- an effort that has often been justified as being in the interest of national security. However, this growth has also brought about questioning of the possibility of uncontrolled government power and the resultant loss of civil liberties, especially the protection of privacy in the Constitution. The shape and validity of state surveillance in Nigeria are thus bargained within the complex structure of law and administrative custom, governed by various security and intelligence services.

4.1 Relevant Laws and Security Agencies

Nigerian legal framework provides state monitoring and intelligence gathering mainly through laws designed to maintain national security, crime and protection of the people. Most of such laws give very wide, loosely defined authorities to security agencies, frequently without any form of strict procedural safeguards or judicial oversight. A principal instrument is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. Section 38 of the Act gives the law-enforcement agencies the right to intercept, monitor and record electronic communications in instances where they consider it necessary to do so based on national security or criminal investigation.[15] The provision allows collecting data in real time and provides the service providers with an obligation to enable access by security agencies. Crucially, however, the statute says nothing about the necessity of prior judicial authorisation, the imposition of time limits, or threshold requirements, thereby leaving broad discretionary scope for implementation.[16]

Another significant measure is the Terrorism (Prevention and Prohibition) Act 2022. This act authorizes intelligence collection, surveillance, and wiretapping in the counter-terrorism situation. Section 28 of the Act grants the Office of the National Security Adviser (ONSA) and the Department of State Services (DSS) authority to gather information and intercept communications suspected of linking to terrorist activities.[17] While the Act mandates Attorney General approval for certain surveillance actions, the absence of publicly accessible oversight reports or judicial challenges complicates any assessment of the legality and proportionality of these operations.[18] Under the National Security Agencies Act 1986, Nigeria's principal intelligence agencies, the Department of State Services (DSS), the National Intelligence Agency (NIA), and the Defence Intelligence Agency (DIA), are established. Their mandate is to collect information that is critical to the national security and defence but the enabling statute fails to define specific confines, internal

[14] C. Eze, "The Nigerian Communications Commission and the Protection of Consumer Data: Regulatory Challenges" *Nigerian Journal of Communications Law and Policy* [2020] (5) (2) 28.

[15] Cybercrimes (Prohibition, Prevention, etc.) Act 2015. s 28

[16] A. Adeoye, "A Legal Review of Interception Powers under Nigeria's Cybercrimes Act" *Journal of Law, Technology and Society* [2022] (4) (2) 63.

[17] Terrorism (Prevention and Prohibition) Act 2022. s 28

[18] M. Muhammed, "Balancing National Security and Civil Liberties in Nigeria's Counter-Terrorism Framework" *Nigerian Journal of Security Law* [2023] (6) (1) 51.

governance and reporting requirements. Consequently, the agencies often operate in relative secrecy, and the scope of their surveillance activities eludes both public oversight and legislative scrutiny.[19]

The Nigerian Communications Commission (NCC), not formally designated a security agency, nonetheless facilitates surveillance by enforcing SIM card registration, data retention, and compliance requirements on telecommunications operators. The Lawful Interception of Communications Regulations 2019, issued by the NCC, permits the authorised interceptions by the government in specified cases. Noteworthy, the regulation lacks independent oversight provisions and fails to mandate prior judicial warrants, diverging from international best practices.[20] Furthermore, the Nigeria Police Force (NPF), especially through its intelligence and cyber-crime units, increasingly employs electronic surveillance during investigations. The absence of coordinated procedures and clearly demarcated jurisdictions often leads to overlapping mandates and jurisdictional disputes, thereby complicating accountability.[21]

4.2 Challenges of Oversight and Accountability

The greatest issue within the Nigerian surveillance system is the lack of open supervision and proper accountability. In democratic states, the power of surveillance is usually controlled by judicial checks, checks by legislatures, and independent regulatory bodies. In Nigeria, however, the current structure is failing on all levels. Judicial supervision is either weak or non-existent. The majority of laws that have been enacted to authorise interception, such as the Cybercrimes Act and the Terrorism Act, do not require prior court authorisation and do not provide any ex post facto judicial oversight of surveillance operations. By contrast, jurisdictions such as the United States and the United Kingdom employ specialised courts to evaluate the necessity and proportionality of state surveillance, with the United States' Foreign Intelligence Surveillance Court (FISC) and the United Kingdom's Investigatory Powers Tribunal serving as models.[22] The fact that there is no such body in Nigeria creates a significant gap that undermines due process.

The parliamentary oversight is, also, very minimal. According to the laws, committees of the National Assembly can summon and interrogate security agencies, but this is rarely done with any degree of seriousness due to political influences, lack of technical know-how and inaccessibility of intelligence activities. Relative to this, legislatures in South Africa and Canada have the authority to conduct classified reviews of the security policies and activities, a power that is notably absent in the Nigerian legislature.[23] After detailed review of the 2023 Nigeria Data Protection Act (NDPA), three principal deficiencies emerge: insufficient institutional accountability mechanisms, limited engagement of civil society and public awareness of surveillance issues, and the absence of effective remedies for victims of unlawful surveillance.

To begin with, institutional accountability mechanism is not well defined. Although the NDPA establishes the Nigeria Data Protection Commission (NDPC) as the regulatory authority for data protection, the Commission's oversight over security agencies is ambiguous. The Act in section 30 gives exemptions to processing of personal data when required on grounds of national security and in effect takes the activities out of the supervision of the NDPC. This restriction reduces the ability of the Commission to make security organizations responsible in cases of violation of privacy of data.

[19] E. Okon, "Secrecy and Surveillance: Rethinking the Legal Framework for Nigeria's Intelligence Agencies" *African Journal of Constitutional Law* [2022] (5) (3) 88.

[20] C. Eze, "The Nigerian Communications Commission and the Protection of Consumer Data: Regulatory Challenges" *Nigerian Journal of Communications Law and Policy* [2020] (5) (2) 28.

[21] F. Okoye, "Navigating Nigeria's Data Protection Act 2023: Rights, Obligations and Exemptions" *African Journal of Cyber Law and Digital Rights* [2024] (2) (1) 18.

[22] L. Donohue, "Bulk Metadata Collection: Statutory and Constitutional Considerations" *Harvard Journal of Law & Public Policy* [2015] (38) (1) 3.

[23] O. Bamgbose, "Parliamentary Oversight of Intelligence Services in Nigeria: Prospects and Pitfalls" *Journal of African Legal Studies* [2021] (4) (1) 22.

Second, the involvement of civil society and common knowledge about surveillance is rather low. When the legal recourses and rights of citizens to privacy are not adequately publicized and when courts are not inclined to rule on such cases, illegal spying often stands unopposed. Human rights organisations have tried to sue privacy infringement in vain due to procedural hurdles or direct rejection by the courts that do not want to get involved in national security issues.[24] Third, the remedies that are available to the victims of illegal surveillance are minimal. Although the Constitution can be used to redress through Section 46, it is not easy to prove that one has had his or her privacy violated, more so where the surveillance was not evident and there was no legal obligation to notify. It is a legal invisibility that strengthens impunity and disempowers individuals who are affected.[25] Fourth, lack of a specific data retention policy in all sectors has contributed to discrepancies in the practices of telecommunications operators and service providers who retain user data indefinitely or respond to requests to access data without the necessary authorisation. Such a backdrop contributes to the threats of data abuse and undermines the trust in digital services among users.[26]

The Nigerian surveillance system presents itself in the form of a combination of far-reaching statutory authorities, poor legal definitions, insufficient safeguards, and poorly equipped institutional oversight. Such gaps create an environment where abuse of power and invasion of privacy in the name of national security can take place. It is in the wake of these deficiencies that Nigeria needs to put in place a rights-based, transparent and accountable surveillance regime. Reforms must include amending the current legislation to require judicial authorisation, periodic review of legislation, specific reporting requirements, and a strong independent oversight mechanism. Besides, it is essential to enhance the capacity of the National Data Protection Commission and define its jurisdiction over the data processing related to security. The call for a comprehensive change in the law is ultimately not enough, but also political will and civic engagement is necessary in the construction of a surveillance system that upholds the rule of law and human dignity.

5. Comparative Perspectives

The attempts of Nigeria to balance the rights of individuals to privacy and the national security requirements require a comparative approach to the strategies used by other jurisdictions. The European Union, the United States, and the United Kingdom, which are facing serious security threats, have developed different regulatory frameworks to align state surveillance with the civil liberties and constitutional safeguards. Analysing these models, it is possible to see various ways of striking a balance between security goals and privacy protection.

5.1 European Union: GDPR and Human Rights Protections

The European Union (EU) constitutes one of the most privacy-oriented jurisdictions on a global scale. The Union's data-privacy framework is built on the premise that privacy constitutes a fundamental human right, a premise codified in Article 8 of the Charter of Fundamental Rights of the European Union and in Article 8 of the European Convention on Human Rights (ECHR). Both instruments state that individuals have the right to protection of their personal data and the right to protection of their personal life, in the event that restrictions are lawful, necessary and proportionate. The General Data Protection Regulation (GDPR), introduced in 2018, has established a benchmark for data governance. The GDPR requires organisations to be transparent, limit their purposes, and minimise their data, and be accountable through principles of transparency, purpose limitation, data minimisation, and accountability. Even though the GDPR does not apply to actions beyond the reach of EU law, most notably intelligence activities, member-state privacy

[24] F. Okoye, "Navigating Nigeria's Data Protection Act 2023: Rights, Obligations and Exemptions" *African Journal of Cyber Law and Digital Rights* [2024] (2) (1) 17.
[25] D. J. Solove, *Understanding Privacy* (Harvard University Press, 2008) 24.
[26] T. Olatunji, "Surveillance and the Right to Privacy in Nigeria: A Legal Analysis" *Nigerian Journal of Cyber Law and Data Protection* [2022] (1) (2) 33.

regulations must conform to fundamental rights standards established by both the Charter of Fundamental Rights and the ECHR.[27]

Strict oversight of surveillance has been supported by the jurisprudence of the ECJ. In *Digital Rights Ireland Ltd v Minister for Communications*,[28] the Court of Justice of the European Union (CJEU) deemed the Data Retention Directive unlawful for disproportionately encroaching on privacy. A parallel judgment in *La Quadrature du Net and Others v Premier Ministre,*[29] determined that general, indiscriminate retention of telecommunications data by intelligence agencies conflicts with EU law. Collectively, the judgments are used to give a doctrinal image of surveillance: any interference must be strictly necessary and proportionate and it must happen under the control of an independent adjudicatory body. Although national security interests warrant attention, they cannot serve as an unbounded rationale for extensive data collection absent judicial or legislative scrutiny.[30] This EU law tradition of rights protection and institutional responsibility can provide good precedents to follow by Nigeria, especially when its plans include strengthening court supervision and reducing any overly broad exemptions in the Data Protection Act 2019.

5.2 United States: The Patriot Act, FISA, and Fourth Amendment Protections

In the United States, there is a heightened relationship between national security issues and surveillance activities especially following the September 11, 2001 terrorist attacks. The USA PATRIOT Act 2001 granted more authority to the intelligence and law-enforcement agencies to tap communications, obtain financial records and track internet activity. Notably, the statute's Section 215 (now expired) allowed the National Security Agency (NSA) to conduct bulk collection of telephone metadata, later revealed by whistle-blower Edward Snowden. These actions led to a strong constitutional argument on the Fourth Amendment protection against the unreasonable searches and seizures. Although surveillance for foreign intelligence purposes falls under the Foreign Intelligence Surveillance Act (FISA) 1978, the proceedings occur in secrecy through the FISA Court (FISC), which authorises wiretaps, data collection, and surveillance with minimal adversarial involvement or public transparency.[31]

In the U.S. federal case *American Civil Liberties Union v. Clapper*,[32] a district court determined that the bulk metadata collection programme exceeded the authority afforded by Section 215 and likely violated constitutional privacy rights. There have been a series of reforms since then, such as the USA FREEDOM Act 2015, but critics say that U.S. surveillance laws continue to allow broad collection of data with limited meaningful oversight. In contrast to the EU, whose privacy policy conceptualizes privacy as a social good, the United States tends to perceive data privacy as a consumer-protection issue that is divided into sector-specific regulations and court precedents. However, the history of the U.S. experience shows that surveillance creep is a dangerous phenomenon when the checks and balances are lax and transparency is low. In the Nigerian legislative system, similar to the USA PATRIOT Act, the surveillance authorities are broad and the state has access to a lot of personal information without having to go through the procedural judicial authorisation stipulated by the FISA. The introduction of a special, separate, independent judicial system (like in the U.S.) would help to bring more clarity to law, and be more constitutively compliant.

5.3 United Kingdom: Investigatory Powers and Safeguards

The 2016 Investigatory Powers Act (IPA) represents a salient illustration from the United Kingdom, often characterised as the "Snooper's Charter." The Act merged existing surveillance powers and added new

[27] B. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) 95.
[28] (Joined Cases C-293/12 and C-594/12) [2014] ECLI:EU:C: 2014:238.
[29] (Joined Cases C-511/18, C-512/18 and C-520/18).
[30] C. Murphy, "Surveillance and the Rule of Law: A Report on the UK Investigatory Powers Act 2016" *Cambridge Law Journal* [2017] (76) (2) 372.
[31] L. Donohue, "Bulk Metadata Collection: Statutory and Constitutional Considerations" *Harvard Journal of Law & Public Policy* [2015] (38) (1) 3.
[32] 785 F.3d 787 (United States Court of Appeals, Second Circuit, 2015).

capabilities in bulk data collection, interference of equipment and a long-term retention of metadata. Intelligence entities such as GCHQ and MI5 now enjoy enhanced investigative capabilities, yet the legislation introduces a "double-lock" oversight regime wherein both ministerial authorisation and scrutiny by Judicial Commissioners is obligatory.[33] Moreover, the Investigatory Powers Tribunal provides a special adjudicative body to which claims of unlawful surveillance can be brought. The UK model aims to establish a balance between good investigatory discretion and good procedural protection. Despite the fact that the IPA has been criticized to have enabled mass surveillance activities, the judicial adjudication has always maintained that it is legal based on procedural safeguards. In *Big Brother Watch v United Kingdom*,[34] the European Court of Human Rights considered the IPA's oversight architecture a noteworthy improvement, albeit expressing apprehension regarding the potential deterrent effects of indiscriminate data collection.

On the other hand, Nigeria lacks equivalent judicial and institutional mechanisms. There are no previous judicial authorisation or independent warrant review or specialised oversight correspondents, thus undermining transparency and democratic oversight. A multi-layered model of oversight, which integrates executive, judicial and independent elements, would help to significantly improve transparency and accountability in the surveillance architecture of Nigeria. In addition to procedural protection, the United Kingdom has systems of institutional transparency, in particular transparency reports that disclose aggregate metadata requesting surveillance. Such tools encourage the confidence of the population and drive legislative oversight. Similar steps would probably be beneficial to Nigeria with a special emphasis on enhancing civic control and democratic accountability.

Comparative equilibrium in Europe Union, United States and United Kingdom depicts divergent equilibria between the competing interests of privacy and security, both of which are motivated by different legal traditions, institutional capacities and popular expectations. The EU has a rights-based model based on human dignity and judicial restraint; the American sensibility leans more towards national security but is also subject to new judicial constraints and institutional changes; the UK has a wide intelligence power coupled with formal protection and oversight. The legal regime in Nigeria, in its turn, lacks the appropriate subtlety. The power of surveillance is widely distributed with a vague definition and judicial and legislative oversight is not well developed. By incorporating precedents of these jurisdictions, Nigeria may be in a position to build a surveillance mechanism that is not only balanced, open, and constitutionally compliant, but also one that protects the right to privacy and allows national security agencies to conduct their operations with ease. The individual lessons are that there must be prior judicial authorisation of surveillance, that special oversight tribunals be set in place, that there is transparency in reporting and that national laws are brought into harmony with international human rights law. With the ever-changing digital environment in the world, these reforms are necessary in guaranteeing the ongoing dedication of Nigeria to its people, and to the rule of rule.

6. Striking A Balance: Privacy Versus Security

6.1 Key Tensions and Legal Dilemmas

The balancing of the right to privacy with the national security requirements is one of the main legal and policy predicaments in the digital era. The two interests are essential to democratic governance but where they meet, the relationship is often tensed. The supporters of data privacy rights stress that the individual should have the right to the use of his or her personal information, and the proponents of national security have to have access to the data in order to prevent crimes, collect intelligence, and counter-terrorist activities. One of the inherent legal issues is related to the extent and the restrictions of state surveillance powers. Numerous statutes in Nigeria and other jurisdictions provide broad exemptions from data protection

[33] C. Murphy, "Surveillance and the Rule of Law: A Report on the UK Investigatory Powers Act 2016" *Cambridge Law Journal* [2017] (76) (2) 372.

[34] [2021] ECHR 581, Applications Nos. 58170/13, 62322/14 and 24960/15 (European Court of Human Rights, 25 May 2021).

principles on national-security grounds, often accompanied by inadequate safeguards or deficient independent oversight.[35] Lack of a clear definition of national security in Nigeria creates a situation of ambiguity that allows broad surveillance activities that could be against constitutional rights. There is an extra difficulty of proportionality and necessity. Legal standards requiring surveillance to be the least intrusive means of achieving security objectives are under-developed or poorly enforced in Nigeria,[36] prompting concerns about arbitrary or disproportionate intrusions into citizens' private lives.

6.2 Lessons from International Jurisdictions

The international legal trends provide valuable advising concerning the negotiation of the conflict between privacy and security. In Digital Rights Ireland, the European Court of Justice reaffirmed the incompatibility of blanket data retention schemes that do not include sufficient safeguards with fundamental rights pursuant to the Charter of Fundamental Rights of the European Union. Similarly, the European Court of Human Rights in *Big Brother Watch v United Kingdom*[37] has echoed the same view by indicating that legal frameworks should have prior judicial authorisation and effective oversight measures. In the United States, *American Civil Liberties Union v. Clapper*,[38] judicial review ultimately resulted in a judicial restriction of the bulk metadata collection of the National Security Agency, proving that the courts are capable of reining in surveillance abuses even in the most securitized contexts. Despite the fact that the U.S. is still being accused of lacking an overall privacy protection law, the legal culture of judicial oversight and legislative change, which is reflected in the tools like the USA FREEDOM Act, promises the gradual change toward more harmonious solutions.

By contrast, the European Union's General Data Protection Regulation (GDPR) offers a sophisticated model of data protection, harmonizing strong individual rights with narrow, clearly defined exceptions permitting public interest and national security priorities. Data minimisation, purpose limitation and independent supervision are also requirements of the GDPR, and these principles could be implemented in Nigeria to strengthen its legal framework.[39] Finally, absolute privacy or absolute security will never be achieved, and it is not even desirable; however, a rights-respecting balance is still possible with the help of well-defined legal standards, judicial checks, transparency, and a sense of accountability. Nigeria has a lot to learn in terms of the adoption and adaptation of the best practices that exist in other parts of the world in order to improve its legal response to the competing demands of privacy and security.

7. The Way Forward for Nigeria

7.1 Legal and Policy Recommendations

Legal, institutional and societal changes are necessary on a wide-scale to address national security needs of Nigeria and its adherence to modern standards of data-protection. First, the Nigeria Data Protection Act 2023 will have to be amended to introduce clear restrictions and strong judicial protections concerning the access to data in the interest of national security. Surveillance authorisations must be subject to prior judicial oversight and narrowly tailored to precise, legitimate security objectives.[40]

[35] O. Ojo, "The Constitutional Right to Privacy and Surveillance Practices in Nigeria" *Nigerian Journal of Human Rights Law* [2021] (3) (1) 44.
[36] A. Adeoye, "A Legal Review of Interception Powers under Nigeria's Cybercrimes Act" *Journal of Law, Technology and Society* [2022] (4) (2) 63.
[37] [2021] ECHR 581, Applications Nos. 58170/13, 62322/14 and 24960/15 (European Court of Human Rights, 25 May 2021).
[38] 785 F.3d 787 (United States Court of Appeals, Second Circuit, 2015).
[39] F. Okoye, "Navigating Nigeria's Data Protection Act 2023: Rights, Obligations and Exemptions" *African Journal of Cyber Law and Digital Rights* [2024] (2) (1) 17.
[40] F. Okoye, "Navigating Nigeria's Data Protection Act 2023: Rights, Obligations and Exemptions" *African Journal of Cyber Law and Digital Rights* [2024] (2) (1) 17.

7.2 Institutional Reforms and Public Oversight

Second, there is the statutory framework which requires strengthening. The Nigeria Data Protection Bureau (NDPB) and the Nigerian Communications Commission (NCC) should be granted greater independence and enforcement capacity to supervise both public and private actors involved in data processing.[41] Accountability would be further increased by creating a special watchdog, similar to Investigatory Powers Commissioner in the UK.

7.3 Enhancing Civic Awareness and Data Protection Culture

Third, digital literacy and awareness should be emphasised. Most Nigerians do not know their privacy rights and this makes them vulnerable to illegal data conduct. Civic education campaigns and the integration of data-protection principles into school curricula can fosters a stronger culture of rights protection.[42] Finally, the rights-based, transparent and participatory approach to the issue is vital in gaining the trust of the people and preventing the legal response of Nigeria to the security threats to undermine the fundamental freedoms.

8. Conclusion

The expanding Nigeria data privacy and national security collision is a legal and policy problem of considerable complexity. Despite the fact that the state can have a valid and strong reason to protect national security, these actions should be balanced with constitutional and international obligations to uphold right to privacy. The current debate shows that the current legal and institutional framework in Nigeria provides a skeletal framework, but it fails to provide transparency, control and accountability. The effectiveness of sound judicial controls, data minimalization and strong regulators is highlighted by comparative models of the European Union, the United States and the United Kingdom. To further the discussion, Nigeria could use a more explicit legal criterion, strengthening of institutional autonomy, and increase in the awareness of data-related rights among the population. A rights-based, balanced framework is the only way to provide legal surveillance, instil trust among citizens and maintain democratic principles in the digital age.

[41] A. Adeoye, "A Legal Review of Interception Powers under Nigeria's Cybercrimes Act" *Journal of Law, Technology and Society* [2022] (4) (2) 63.

[42] O. Ojo, "The Constitutional Right to Privacy and Surveillance Practices in Nigeria" *Nigerian Journal of Human Rights Law* [2021] (3) (1) 44.