UNIZIK LAW JOURNAL 19, (3) 2023

APPRAISING THE INSTITUTIONAL FRAMEWORKS FOR PROTECTION OF RIGHTS TO PRIVACY IN NIGERIA VIS-À-VIS UNAUTHORIZED WIRETAPPING OF TELEPHONE COMMUNICATIONS**

Abstract

The incessant wiretapping of citizen's telephone conversation and some other telecommunications in Nigeria has not only constituted serious fundamental rights issues relating to the rights to private and family life but is also plunging the country into a state of anarchy where politicians at the Federal, State and Local government level, powerful or highly connected individuals, invade into citizens' privacy without justification and due process. The network service providers are also culprits in this act as they perpetrate these acts unchallenged and aid the security agencies and private individuals in carrying out unauthorized wiretapping. The continuous breach undoubtedly stems from the incomprehensive legal framework for the protection of data especially as it relates to telephone communication. The consequences include but not limited to the breach of citizens' fundamental human rights. This article is aimed at appraising the rights to privacy in Nigeria especially as it relates to unauthorized wiretapping *vis-a-vis* the efficacy or otherwise of the institutional framework for the protection of data privacy rights. In a bid to achieve that, the authors adopted the doctrinal method of research which entails the use of books, journals, articles, statutes, case laws and materials. This article found that there is reckless infringement of privacy rights in Nigeria by security agencies, service providers and even individuals. The article also found that there is deficient legal framework for the protection and regulation of wiretapping given rise to inefficient institutional framework for the protection of such rights. The article recommended for the review of and enactment of privacy legislations especially as it relates to protection against wiretapping and stipulation of strong sanctions for breach of privacy rights. It is further recommended that the courts and other institutions should also be strengthened in order to monitor, implement, regulate, interpret and prosecute and sanctions offenders.

Keywords: Rights, Privacy, Telecommunication, Unauthorised Wiretapping, Institutional Framework

1. Introduction

The ability to freely articulate thoughts without hesitation is a fundamental human right.[1] In Nigeria, the Constitution safeguards citizens' rights to express themselves without restraint provided it does not inflict harm upon individuals or groups. Nevertheless, since the inception of language and personal conversations, eavesdroppers have endeavoured to intercept private discussions. The Nigerian proverb, "the wall has ears," symbolizes this concept of covert listening, with eavesdroppers figuratively slipping within the "eaves" to eavesdrop on confidential conversations. With technological progress, eavesdropping has become more convenient through wiretapping.

Section 37 of the Nigerian Constitution explicitly provides for the protection of the privacy of Nigerian citizens, their homes, correspondence, telephone conversations and

* **Ogugua VC Ikpeze, PhD**, Professor and Dean, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria, ovc.ikpeze@unizik.edu.ng, diaikpeze@yahoo.com; Tel. No: 234-8068733216

** **Chukwunonso Augustus Aniekwe,** LLB, BL, LLM (Unizik, Nigeria), LLM (University of Bolton, UK-in view), PhD Candidate, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. Tel: +234 806 6922 005, +44 775 2632 729, justiceaniekwe@gmail.com

[1] B Adémólá-Olátéjú, 'Eavesdropping, Censorship and The Voyeuristic State' (2021) https://www.premiumtimesng.com/opinion/473323-eavesdropping-censorship-and-the-voyeuristic-state-by-bamidele-ademola-olateju.html?tztc=1 Accessed 12 September 2023.

telegraphic communications.[2] However, the constitution does not clarify the mechanism for the protection of that privacy. In 2019, the Nigerian Communications Commission published the "Lawful Interceptions of Communications Regulations 2019," an adjunct to the Nigerian Communications Act of 2003.[3] These regulations empower law enforcement agencies to intercept communications provided by communication licensees.[4] Authorised agencies must first obtain a warrant from a judge, requiring the licensee to:

a) Intercept any communication as described in the warrant.
b) Disclose intercepted communications.
c) Assist foreign authorities in accordance with an international mutual assistance agreement.

Warrants are permissible for specific purposes, including:

a) It is in the interest of national security as directed by the Office of the National Security Adviser or the State Security Services.
b) For the purpose of preventing or investigating a crime.
c) For the purpose of protecting and safeguarding the economic wellbeing of Nigerians.
d) In the interest of public emergency or safety.
e) Giving effect to any international mutual assistance agreements, to which Nigeria is a party.

The provisions of the Lawful Interceptions of Communications Regulations, 2019 amongst others, poses a great threat to the enforcement of the rights of privacy of citizens guaranteed under the 1999 Constitution of Nigeria, leading to grave conflict of laws. However, as the Nigerian telecommunications revolution progressed, crimes are being committed using electronic devices, particularly mobile telephones and computers. In attempting to solve some of these crimes, law enforcement agencies have found call records of targeted individuals useful, and obtained them to speed up investigations. In many cases, these have not been done with warrants duly signed by judges of competent courts.

Section 12 (4) of the regulation allows interception of communications without a warrant. It provides that

> Notwithstanding the provisions of these Regulations, an authorised agency may initiate interception of Communications without a warrant in the event of—
> (a) immediate danger of death or serious injury to any person;
> (b) activities that threaten the national security; or
> (c) activities having characteristics of organised crime;
> provided that the Authorised Agency shall apply for a Warrant to the Judge within 48 hours after the interception has occurred or began to occur before issuance of a Warrant for such interception and where the application is not made, or denied within 48 hours, the interception

[2]Constitution of the Federal Republic of Nigeria 1999 (as amended), Section 37.
[3]Federal Republic of Nigeria Official Gazette, No. 12, 23 January 2019, Vol. 106.
[4]O Oyewole, 'Lawful Interception of Communications under the Nigeria Communications Act and the Peculiarities of the NITDA Draft Code Of Practice For Interactive Computer Platform/Internet Intermediaries", https://www.mondaq.com/nigeria/telecoms-mobile--cable-communications/1217040/lawful-interception-of-communications-under-the-nigeria-communications-act-and-the-peculiarities-of-the-nitda-draft-code-of-practice-for-interactive-computer-platforminternet-intermediaries, Accessed 12 September 2023.

> shall terminate immediately and further interception shall be treated as unlawful.

We hold that this is not just porous as it is open to all kinds of abuses, but injurious to the privacy and privacy of communications among individuals.

Further, the regulation says in Section 14 that:

> A warrant shall be granted for an initial period of three months or such lesser period as the judge may determine based on the circumstances of the application made before the judge and shall cease to have effect at the end of the period stipulated in the warrant unless renewed.

This is particularly problematic, as information accumulated over three months may not be germane to the initial case but form grounds for a fresh case. This cannot be overlooked in a polity like ours, where public institutions are prone to misuse and abuse by elected officials in pursuit of political objectives. Our communications are on record, and fears abound that under the cover of fighting crimes, the records can be used for other purposes. A solution could be found in provision of jail terms for those who abuse information collected for national security or for crime investigation. Section 37 of the Constitution states that, 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.'

It is a fact that the Lawful Interception of Communications Regulation operates on the strength of Section 45 of the Constitution. It grants authority to authorized agencies to intercept any communication where the interception relates to the use of a communications service provided by a licensee to persons in Nigeria; or the interception relates to the use of a Communications Service provided by a licensee to a person outside Nigeria.[5] The Regulation in Section 8 further provided for when there can be an interception without a warrant. This includes when one of the parties consents to the interception, when it is done by a person who is a party to the communication and has sufficient reason to believe that there is a threat to human life and safety; and, in the ordinary course of business, it is required to record or monitor such communication.

However, this lacuna was generally captured in Section 45 of the Constitution which provides that: Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom of other persons. Interpreting the above section 45, the implication is that a law can make provisions to provide for when interception of communication can be lawful, despite the provisions of the Constitution. The only requirement that a law has to meet is that the purpose of such law (interception) is for the purpose of defence, public safety, public order, public morality, public healthy; or for the purpose of protecting the rights and freedom of other persons.

The Lawful Interception of Communications Regulations is clearly geared towards the wordings and intent of Section 45 of the Constitution. The reasons provided by the

[5] *Ibid*. Section 4

Regulation vividly reveals that the essence of the interception is for the purpose of public safety, public order; or for the purpose of protecting the rights and freedom of other persons.[6]

The provisions of the Lawful Interceptions of Communications Regulations 2019 is derogation to the enforcement of the fundamental rights to privacy. The Lawful Interception of Communication Regulation amongst others, poses a great threat to the enforcement of the rights of privacy of citizens guaranteed under the 1999 Constitution of Nigeria, leading to grave conflict of laws. The Regulation therefore, runs contrary to the Constitution, without appropriate checks against abuses, it will pose more dangers by curtailing our liberties than in fighting crimes. Good enough, *Nigeria Communication Commission (Registration of Telephone Subscribers Regulation 2011) in Sections 9 and 10 of the 2011 Regulation, provide confidentiality for telephone subscribers' records maintained in the NCC database. The regulation also gives subscribers the right to view and update personal information held in the NCC central database of a communication company, the enforcement of these provisions leave much to be desired, as it seems only applicable in principle.* Thought the Act introduced laudable provisions, unfortunately, the Act did not make any mention of wiretapping but only provided for the licensing and regulation of network service providers and the telecommunications industries in Nigeria.

The NITDA Act empowers the National Information and Technology Agency (NITDA) to set down guidelines to cater for electronic governance and monitoring the use of electronic data exchange. The Act also empowered the Agency to develop and issue with the erstwhile Data Protection Regulation 2019. The NITDA Regulation seeks to safeguard the rights of natural persons to data privacy, foster the safe handling of transactions involving the exchange of personal data, prevent acts of data manipulation, and ensure Nigerian businesses remain competitive in the international marketplace through the adoption of legal and regulatory frameworks which secure personal data and meet international standards. These provisions, though laudable but did not address the issues of wiretapping. Although the NITDA Act came close it with when it amongst others empowered the NITDA to monitor and govern electronic data exchange, and provided punishment for breaches, but did not provide a practicable enforcement mechanism against the service providers.

The provisions of National Security Agencies Act 1986 disengaging the Nigerian Security Organisation and to creating three security agencies: the Defence Intelligence Agency; the National Intelligence Agency. and the State Security Service is criticized by the authors not only for being bogus in its scope and mode of application in that there are no clear definitions as to the ambit of the powers and functions of the security agencies seeing as most of their functions are tied to the discretion of the President, but also the fact that the Act violates the Constitution and contradicts with section 1, chapter IV and section 37 of the Constitution as it particularly relates to the processing of personal data. This contravention is made manifest by the provisions of section 1(4) of the NSA Act which provides that the provisions of subsections (I), (2) and (3) of this section shall have effect

[6] O Nwakor, Lawful Interception of Communications: An Examination of the Inconsistency or Otherwise of Section 39 of the Cybercrime (Prohibition, Prevention, Etc) Act, 2015 with Section 37 of the 1999 Constitution of the Federal Republic of Nigeria, file:///C:/Users/USER/Downloads/SSRN-id4524093%20(1).pdf, accessed 18 November 2023

notwithstanding the provisions of any other law to the contrary, or any matter therein mentioned. Similar provisions apply in the SSS Instrument No. 1 of 1999 which has become a subject of controversy in that the decree has no regulation whatsoever and is purportedly ranked over Nigeria's Constitution and also leaves the President with excessive powers to determine the operations of the SSS as the President deems fit. It is, therefore, the position of the writer that these laws be amended to ensure that it guarantees the protection of the rights of data subjects in Nigeria.

It is most unfortunate that most legislations and regulations protecting privacy, enacting securities agencies, establishing and regulating network service providers, did not address sufficiently against wiretapping, not even the *grund norm*, being the 1999 Constitution of the Federal Republic of Nigeria (as amended) as it did not even define privacy or what constitute same. The Lawful Interception of Communication Regulation which came too close to addressing the issues of wiretapping, still left a lot of loopholes and susceptible to abuse by the government of the day as well as security agencies and network service providers. The article therefore discussed the institutional framework for the protection of data privacy rights in Nigeria as follow:

2. Institutional Framework for the Protection of Privacy and Data Rights in Nigeria

2.1 Nigeria Data Protection Commission

The Nigerian Data Protection Commission (NDPC) was created pursuant to the provisions of the Data Protection Act (NDPA) 2023. The transitional provision confers all the powers and duties of the formerly existing Nigerian Data Protection Bureau to the Commission. In the case of violation of a data subject's rights to privacy, Section 48 of the NDPA states that the NDPC may also issue enforcement orders, including requiring the Data Controller or Data Processor to remedy the violation, ordering the Data Controller or Data Processor to pay compensation to a Data Subject; ordering the Data Controller or Data Processor to account for the profits realized from the violation or harm as a result of a violation; or referring the matter to the appropriate regulatory agencies for sanction and to prosecute the organization.

The NDPC may also institute criminal proceedings where it has determined that an organization is in breach of the provisions of the NDPA or NDPR, especially where such breach affects national security, sovereignty, and cohesion. The NDPC may also seek a fiat of the Honourable Attorney General of the Federation or may file a petition with any authority in Nigeria. This may include the Economic and Financial Crimes Commission; the Department of State Security; the Nigerian Police Force; the Independent Corrupt Practices (and other related offenses) Commission; or the Office of National Security Adviser. At its core, the Bureau is entrusted with the mandate to work in collaboration with stakeholders to achieve the strategic objectives of the NDPR, which encompass:

a) Safeguarding the inherent data privacy rights of individuals.
b) Facilitating secure and trustworthy transactions involving the exchange of Personal Data.
c) Preventing unauthorized manipulation of Personal Data.
d) Ensuring the sustained global competitiveness of Nigerian businesses through a just and equitable legal framework for data protection that aligns seamlessly with established best practices.

It is unfortunate to note from the intendment of the Data Protection Act that is more or less made to protect the interest of the State. This evident for instance in the fact that Act only empowers the Commission the power to bring action against any organization who is in breach, especially where such breach affects national security, sovereignty, and cohesion The Act did not expressly provide for safeguards against wiretapping of telephonic communication neither did it envisage the incidence of breach of data privacy by the State or machineries of the State and the remedy available to the citizen. The effect therefore is on the institution which becomes ineffective in meeting the demands of citizens to enjoy their rights.

2.2 Nigeria Communications Commission

In consonance with the provisions stipulated in Section 70 of the Nigerian Communications Act 2003 (NCA 2003), the Commission is vested with the authority to formulate and disseminate regulations addressing a spectrum of subjects, encompassing, yet not limited to: written authorizations, permits, assignments, and licenses issued under the ambit of the NCA 2003; the allocation of rights to spectrum or numbers; transgressions in the realm of communications and their corresponding penalties; the establishment of fees, charges, rates, or fines; an encompassing framework for universal service provision; benchmarks for upholding Quality of Service (QoS); and any other requisite components for the effective implementation of the NCA 2003's tenets.[7]

To fortify robust data protection, the Nigerian Communications Commission (NCC) has promulgated the ensuing regulations:

2.2.1 Annual Operating Levy Regulations:

These regulations set forth a range of objectives:

(a) To devise and administer an effective regulatory framework for the annual operating levy system by the commission.

(b) To delineate the modes and methodologies for evaluating and disbursing the annual operating levy.

(c) To enunciate guiding principles and benchmarks for the commission's administration of the annual operating levy mechanism.

To fulfil these objectives, the commission has introduced evaluation rates for these levies, established accounting standards tailored to the communication industry, procedures for validating financial statements, evaluations of licenses' annual operating levies, and mechanisms for imposing sanctions and penalties on non-compliant licensees.

2.2.2 Consumer Code Regulations

Positioned as Part I of Chapter VIII of the Nigerian Communications Act, these regulations offer a nuanced explication of the processes and essential requisites governing the development of consumer codes relevant to licensed telecommunications operators in Nigeria alongside interconnected consumer practices. Key objectives of these Regulations encompass:

[7] https://www.ncc.gov.ng/licensing-regulation/legal/regulations Accessed 10 August 2023

(a) Clarifying the prescribed procedures to be adhered to by Licensees when fashioning approved consumer codes of practice in alignment with the dictates of section 106 of the Act.
(b) Defining the essential contents and attributes of any consumer code prepared by, or pertinent to, Licensees.
These Regulations are universally applicable, encompassing all Licensees and any other entities providing communication services within Nigeria.

2.2.3 Lawful Interception of Communications Regulation:

Exercising the authority endowed by section 70 of the Nigerian Communications Act, 2003, and other pertinent powers, the Nigerian Communications Commission endeavors to:
(a) Establish a comprehensive legal and regulatory framework for the lawful interception of communications within Nigeria, in consonance with the provisions outlined in sections 146 and 147 of the Act.
(b) Specify the nature and categories of communications subject to interception.
(c) Prescribe penalties for instances of non-compliance with the Act and these Regulations.
(d) Detail a structured notification procedure for the Commission pertaining to all warrants issued, modified, renewed, or revoked under these Regulations.
(e) Safeguard the privacy of subscribers' communications, consistent with the protections enshrined in the Constitution of the Federal Republic of Nigeria

2.2.4 Universal Access and Universal Service Regulation:

In tandem with Chapter VII of the Nigerian Communications Act, 2003 (2003 No. 19), and their interconnected facets, the overarching objectives of the universal access and universal service provision system encompass:
(a) Elevating social equity and inclusivity for the populace of Nigeria.
(b) Contributing substantively to Nigeria's broader economic, social, and cultural development.
The functions of the Universal Service Protection (USP) Board encompass:
(a) Overseeing and providing overarching policy direction for the management of the USP Fund and the USP Fund Managers.
(b) Appointing and relieving the USP Fund Managers in consultation with the Commission.
(c) Appointing and removing auditors for the USP Fund.
(d) Endorsing Operating Plans encompassing one or more USP Programs and USP Projects, along with a budget for all operations and expenditures of the USP Board, USP Fund Managers, and all endeavours financed by the USP Fund throughout the Operating Plan's duration.
(e) Ratifying standing orders to define and regulate the actions of the USP Fund Manager and amending these orders as needed.
(f) Sanctioning all processes, procedures, guidelines, and determinations necessary for the full implementation of these Regulations.
(g) Executing all additional functions assigned to the USP Board as per the Act and these Regulations.

Despite the abundance of these regulations, a lack of consensus prevails among judicial opinions regarding data privacy, presenting a significant obstacle to effective data

protection in Nigeria. While some courts regard data privacy as an inherent right of the data subject, others interpret it as a right that should be upheld through regulatory oversight, even if the data was initially provided to a company for service provision. Similar to many other common law jurisdictions, judicial decisions carry substantial weight in Nigeria's legal landscape. While relatively scarce, there have been court rulings on matters of data privacy and protection, including notable cases such as *Godfrey Nya Eneye v MTN Nigeria Communication Ltd*[8] and *Barr. Ezugwu Anene v Airtel Nigeria Ltd.*[9] In the case of *Godfrey Nya Eneye v MTN Nigeria Communication Ltd*,[10] Mr. Eneye, a legal practitioner, initiated legal proceedings against MTN Communication Limited. He alleged that MTN had divulged his mobile telephone number to unknown third parties without obtaining his consent, leading to unsolicited text messages being sent to him. He argued that this breach constituted a violation of his fundamental right to privacy, as enshrined in Section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended). He also contended that his rights to freedom of association under Section 40 and liberty under Section 35 of the Constitution had been infringed by MTN. Seeking an injunction to restrain MTN from further unauthorized access to his mobile phone number,

Mr. Eneye claimed that he experienced distress due to disturbances caused by text messages from unknown third parties at any time, especially during work hours and late at night. Additionally, he asserted suffering financial losses as his airtime was deducted from unsubscribing. The court ruled in his favour, holding that the unauthorized disclosure of the claimant's mobile phone number by his telecommunications service provider (the defendant) and subsequent unsolicited text messages from unknown third parties constituted violations of his constitutional right to privacy.

In the case of *Mr. Ezugwu Emmanuel Anene v Airtel Nigeria Ltd*,[11] the plaintiff filed a lawsuit against his service provider, Airtel, at the FCT High Court in 2015. The plaintiff brought forth the action under undefended claims, alleging that the numerous unsolicited calls and text messages from Airtel and third parties, who obtained his number due to Airtel's disclosure, breached his constitutional right to privacy and other related claims. As Airtel did not mount a defence, the court relied on the plaintiff's evidence and rendered judgment in his favour, awarding him five million Naira (N5, 000,000.00) in damages for the violation of his privacy right.

2.3 Defence Intelligence Agency (DIA)

Notwithstanding the fact that the DIA is not concerned with internal affairs, the DIA may be regarded as a data controller due to the fact that it processes information of a wide range and therefore falls within the ambit of this discourse. According to the NDPA, a "Data Controller or Data Processor of Major Importance" is a Data Controller or Data Processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the NDPC may prescribe, or such other class of Data Controller or Data Processor that is

[8] Appeal No: CA/A/689/2013 (Unreported), https://www.refworld.org/pdfid/54f97e064.pdf Accessed 16 August 16 2023.
[9] FCT/HC/CV/545/2015 (Unreported). https://scirp.org/reference/referencespapers.aspx?referenceid=3143231
[10](2013) CA/A/689 (Unreported).
[11]Suit No: FCT/HC/CV/545/2015 (Unreported).

processing Personal Data of particular value or significance to the economy, society or security of Nigeria as the NDPC may designate. Section 39(1) of the NDPA also requires a Data Controller and Data Processor to implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of Personal Data in its possession. The DIA was established under the National Securities Act for the following purposes:

(a). the prevention and detection of crimes of a military nature against the security of Nigeria;

(b). the protection and preservation of all military classified matters concerning the security of Nigeria, both within and outside Nigeria;

(c). such other responsibilities affecting defence intelligence of a military nature, both within and outside Nigeria, as the President, or the Chief of Defence Staff, as the case may be, may deem necessary.

Amidst the weighty responsibility entrusted to the Defence Intelligence Agency (DIA) for preserving the data privacy of its citizens, a disconcerting shadow has been cast over its integrity due to allegations involving potential breaches of data confidentiality. The revealing exposé authored by The Cable newspaper under the title 'Revealed: Defence Intelligence Agency Acquired Equipment to Spy on Calls, SMS in Nigeria' has unveiled a troubling narrative surrounding the DIA's purported acquisition of surveillance equipment designed to intercept calls and text messages exchanged by Nigerian citizens.[12] This alarming disclosure emerges from an investigative report meticulously compiled by Citizens Lab, a multidisciplinary laboratory operating within the esteemed Munk School of Global Affairs and Public Policy at the University of Toronto, Canada. With a resolute focus on unearthing instances of digital espionage targeting civil society, Citizens Lab has spotlighted the intersection of technology, privacy, and national security.

At the heart of their latest dossier titled "Running in Circles: Uncovering the Clients of Cyber Espionage Firm Circles," a disconcerting narrative takes form, casting a sombre light on the actions of Nigeria's premier military intelligence agency—an entity that operates under the direct jurisdiction of the DIA. The disturbing undercurrent of the report insinuates that the DIA might have been implicated in covert surveillance activities involving citizens' communications. Through meticulous analysis and probing investigation, Citizens Lab's findings unveil that the DIA procured access to Signaling System 7 (SS7), an intricate protocol suite originally developed to facilitate the exchange of information and the routing of phone calls across diverse wireline telecommunications companies. Of noteworthy concern, the acquisition of the SS7 system was attributed to a transaction brokered with Circles, a shadowy surveillance entity renowned for exploiting vulnerabilities within the global mobile phone network to surreptitiously intercept phone conversations, text messages, and even track the geographical coordinates of mobile devices. While the exact specifics of concrete instances where Circles' SS7 system was allegedly employed to conduct surveillance activities remain undisclosed within the confines of the Citizens Lab

[12]https://www.thecable.ng/revealed-defence-intelligence-agency-acquired-equipment-to-spy-on-calls-text-messages-by-nigerians, accessed 5 December 2020.

report, the implications of these unsettling allegations loom large, casting an inescapable pall over the DIA's perceived role as a steadfast guardian of data privacy within Nigeria.

The unfolding implications arising from these allegations prompt a thoughtful contemplation of the intricate interplay between imperatives of national security and the sacrosanct rights of individuals to privacy. This revelation underscores an urgent necessity for a transparent and accountable framework that skillfully reconciles the seemingly competing demands of preserving security and upholding citizens' rights, preventing any encroachment upon personal privacy under the guise of safeguarding the nation. As Nigeria charts its course through the labyrinthine landscape of data protection, it becomes increasingly paramount to strike an artful balance between fortifying against external threats and resolutely upholding the fundamental rights of its citizens.

2.4 National Intelligence Agency (NIA)

Much like the DIA, the NIA is also concerned with external affairs affecting the security of the nation. It also processes the data of citizens in the course of the discharge of its duties. Hence, the need to examine its functions and powers in that regard. The NIA was established for the following purposes:

> a. the general maintenance of the security of Nigeria outside Nigeria, concerning matters that are not related to military issues; and
> b. such other responsibilities affecting national intelligence outside Nigeria as the National Defence Councilor, the President, as the case may be, may deem necessary.

Section 41 and 42 of the Nigerian Data Protection Act prohibits data controllers/processors from transferring personal data to other jurisdictions unless the recipient of the personal data is subject to a framework that affords an adequate level of protection of personal data in line with the provisions of the Act. The Nigerian Data Protection Commission is also empowered to determine whether a country, region, or specified sector within a country or standard contractual clause affords an adequate level of protection. The NIA, thus should ensure that they are in full compliance with the provision of the Nigerian Data Protection Act as well as the Nigerian Constitution on the protection of the rights of data subjects, which undoubtedly, they are not presently complying with.

2.5 The State Security Service

Fulfilling one of the promises made in his first national address as president, Babangida, in June 1986, issued Decree Number 19, dissolving the NSO and restructuring Nigeria's security services into three separate organizations under the Office of the Co-ordinator of National Security. The new State Security Service (SSS) was responsible for intelligence within Nigeria. The State Security Service (SSS) is enabled to perform its roles and functions chiefly by SSS Instrument No.1 of 1999 made pursuant to Section 6 of the National Security Agencies (NSA) Act 1986.[13] It is worthy to note that over the years, other decrees (Decree No. 16 of 1976 and Decree 19 of 1986) charged the Agency with roles and functions that

[13]Cap. 74, LFN 2004

are very similar in content.[14] These include but are not limited to the following Prevention and Detection of any crime against the internal security of Nigeria; Protection and Preservation of all non-military classified matters concerning the internal security of Nigeria; and Prevention, Detection, and Investigation of threats of Espionage, Subversion, Sabotage, Terrorism, Separatist agitations, Inter-group conflicts, Economic crimes of National security dimension, and threats to law and order; etc.

It is however unfortunate that the SSS are the chief culprit in the act of wiretapping citizens telephone communication. Their unlimited powers to do to do that are derived from the establishment Acts: the National Securities Act of 1986 and the SSS Instrument No.1 of 1999 whose by its provisions are ranked above the Constitution of the Federal Republic of Nigeria. Until these Acts are reviewed, the protection of the rights of privacy of Nigerians especially as it relates to telephone communication will continue to be a dream.

2.6 Economic and Financial Crimes Commission (EFCC)

The EFCC Establishment Act was first enacted in 2002 and amended in 2004. The Act commissions the EFCC to combat economic and financial crimes, thereby enabling the Commission to prevent, investigate, prosecute and penalize economic and financial crimes. In order to sanitize the system, the agency is also charged with the responsibility of executing the provisions of other laws and regulations that are related to economic and financial crimes.[15] These laws as embedded in Section 7(2) of the Establishment Act 2004 are:

(a) The Money Laundering Act of 1995
(b) The Money Laundering (Prohibition) Act 2004
(c) The Advance Fee Fraud and Other Fraud Related Offences Act 1995
(d) The Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994
(e) The Banks and other Financial Institutions Act 1991
(f) Miscellaneous Offences Act, 1985
(g) The Criminal Code and the Penal Code
(h) Terrorism Act, 2011

In response to international pressure from the Financial Action Task Force on Money Laundering (FATF), which identified Nigeria among the 23 countries not cooperating with global anti-money laundering efforts, the establishment of the Economic and Financial Crimes Commission (EFCC) was a significant step. However, despite its mandate to investigate and prosecute corrupt practices as vested by the EFCC ACT, 2004, there have been persistent concerns and debates regarding the scope of powers attributed to the EFCC. Embedded within Nigeria's multifaceted legal landscape, several critical legal issues have emerged, reverberating with implications that resonate across the federation's federal structure. A foundational query looms: Does the EFCC bear the jurisdictional mantle to delve into and prosecute economic and financial crimes throughout all corners of the nation? Simultaneously, a parallel inquiry questions the EFCC's prerogative in cases involving properties owned by individual constituent states within the federation. These queries are

[14] https://www.dss.gov.ng/dss_about Department of State Services. Accessed 10 August 2023.
[15] https://www.efcc.gov.ng/efcc/about-us-new/the-establishment-act Accessed 10 August 2023.

further compounded by the constitutional framework of a federal system, which inherently grants substantial autonomy to individual states.[16]

In navigating this intricate terrain, the EFCC must constantly strike a delicate balance, striving to be a beacon of integrity while treading the thin line between law enforcement and the preservation of individual liberties. With the advent of digital money lending in recent times, the EFCC has since swung into action to crack down on Digital Money Lenders (DMLs) who resort to all sorts of measures in retrieving loans from defaulting borrowers, including breach of their data privacy rights. These DMLs go as far as getting the consent of unsuspecting individuals to process their personal data for purposes of harassment and sharing with third parties in any event that they do not make good their obligations. This practice is clearly outlawed by the provisions of the NDPA and thus is actionable.

2.7 National Information Technology Development Agency *(*NITDA*)*

As a regulatory Agency, NITDA is the clearing house for all Government Information Technology projects and infrastructural development in the country. The Agency's role, therefore, is to develop Information technology in Nigeria through the use of regulatory instruments. The instruments are designed to achieve the Information Technology policy objectives by providing frameworks within which to implement policies. The instruments serve as a minimum benchmark in the development and implementation of information technology in Nigeria and enforceable by law.[17]

The instruments are being reviewed frequently due to the dynamic nature of the IT environment and technology innovations, namely:

(a) Digital Literacy Framework
(b) NDPR Implementation Framework
(c) Guidelines for The Management of Personal Data by Public Institutions in Nigeria, 2020
(d) Guidelines for Nigerian Content Development in Information and Communication Technology (ICT)
(e) Framework and Guidelines for Public Internet Access
(f) Guidelines for Clearance of Information Technology (IT) Project by Public Institutions
(g) Guidelines for Registration of ICT Service Providers/Contractors for Delivery of It Services to MDAs
(h) Nigeria e-Government Interoperability Framework (Ne-GIF)
(i) Framework and Guidelines for Information and Communication Technology (ICT) Adoption in Tertiary Institutions
(j) Framework and Guidelines for the Use of Social Media Platforms in Public Institutions
(k) Nigerian Government Enterprise Architecture

Amidst the complex landscape of data privacy, the proactive strides taken by the National Information Technology Development Agency (NITDA) by introducing the Nigeria Data Protection Regulation (NDPR) 2019 stand as a commendable endeavour.

[16] https://thenationonlineng.net/appeal-court-slams-efcc-for-abuse-of-power/ Accessed 16 August 2023.
[17] https://nitda.gov.ng/regulations/

However, despite these commendable efforts, the spectre of data privacy concerns continues to cast its shadow, raising critical questions about the sufficiency and comprehensiveness of the regulatory framework.[18] While the NDPR was established with the laudable aim of bolstering data protection in Nigeria, a closer examination reveals certain inherent limitations that warrant careful consideration and potential refinement. A salient example lies within Paragraph 1.0 (a) of the NDPR, which confines the protective provisions of the regulation solely to the rights of natural persons. This means that institutions and businesses, vulnerable to data privacy breaches, misuse, or theft, might find themselves bereft of remedies under the regulation's ambit, should a literal judicial interpretation prevail.

Furthermore, the NDPR's limited protection of electronic data poses an additional challenge. While digital data forms a significant share of contemporary information exchange, the regulation overlooks the broader landscape of data formats, such as physical documents, letters, surveys, and more. In an era where data assumes multifaceted manifestations, this compartmentalized view threatens to undermine the overarching goal of the NDPR to enhance the protective umbrella enshrined in Section 37 of the Nigerian Constitution. The disparity between the regulation's intention and its practical coverage becomes tangible in light of these limitations. The progressive intent of the NDPR to elevate data protection standards may inadvertently fall short of achieving this grand vision. The very limitations meant to channel the regulation's effectiveness could inadvertently undermine its long-term viability, leading to a regulatory cycle marked by revisions and amendments that attempt to rectify these inherent gaps.

An illustrative context is seen in the legal dispute involving NITDA and TrueCaller in 2019,[19] as well as the notable confrontation between NITDA and the Lagos State Internal Revenue Service.[20] In both instances, the private information of Nigerians was inadvertently exposed without consent—circumstances that, by no means, align with the principled goals of data protection. Such instances underscore the criticality of robust data protection mechanisms, especially in a world where data security has transformed into a core component of negotiations among companies spanning diverse jurisdictions. As the currency of data protection wields influence over building trust in business operations and facilitating seamless transactions, it becomes imperative for companies and individuals in Nigeria to possess a firm grasp of the prevailing laws governing data privacy and protection within the nation.

In the midst of this intricate consideration of technological advancement and legal safeguards, the relevance of data protection becomes increasingly pronounced. A robust and enduring framework must emerge, one that harmonizes the imperatives of data privacy with the practical realities of modern information exchange. The NDPR, as a cornerstone of this endeavour, must continuously evolve to embrace the fluidity of data dynamics while preserving the rights and dignity of individuals and entities alike.

[18]A Odusote 'Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation', (2021), *Beijing Law Review*, 12(4).

[19]https://techcabal.com/2019/09/30/the-people-v-big-tech-nigerian-takes-truecaller-to-court-for-alleged-violation-of-privacy-rights/, accessed 18 October 2023

[20] https://businessday.ng/lead-story/article/nitda-says-lirs-breaches-nigeria-data-protection-regulation/, accessed 19 October 2023.

2.8 Courts

Despite the fact that the Evidence Act was revised in 2011 to allow for the admission of electronic evidence, until 2015, effective criminal justice procedures were impeded by the lack of a legal framework for cybercrime.[21] In recent times, however, the courts have recognized the narrative that data privacy rights are subsumed under the right to privacy guaranteed under S. 37 of the Constitution.[22] The Cybercrime Act of 2015 also provides jurisdiction for the courts to prosecute matters relating to cybercrime as it criminalizes certain actions related to cybercrime. While countless cyber attacks on computers and data are logged every day throughout the globe, only a tiny percentage of cybercrime - that is, offenses against and via computers - is prosecuted and judged. Besides that, evidence in connection with any crime is increasingly accessible in electronic form on computer systems or storage devices, and such evidence must be protected for criminal proceedings.[23]

The Nigerian Data Protection Act provides the courts with the jurisdiction to hear matters relating to Data protection. The Act vests powers in the courts to entertain judicial review of orders within 30 days of issuance by the Commission. Data subjects can institute independent civil proceedings to recover damages where the said data subject suffers injury, loss, or harm. The Court may also make an order of forfeiture against a convicted data controller, processor, or individual in accordance with the Proceeds of Crime (Recovery and Management) Act. Furthermore, where an offense has been committed by a body corporate or firm, the body corporate or firm, as well as its principal officers, shall be deemed culpable unless the principal officers prove that the offense was committed without their consent or connivance and they exercised diligence to prevent the commission of the offense.[24] Data controllers and processors will also be vicariously liable for the acts or omissions of their agents or employees. Thus, data protection compliance should be a top priority for principal officers, which include management staff, since they can be held personally liable in the event the organization fails to comply.

3. Conclusion

This article found that there is reckless infringement of privacy rights in Nigeria by security agencies, service providers and even individuals. The continuous breach undoubtedly resulted from the incomprehensive legal framework for the protection of data especially as it relates to telephone communication. The consequences includes but not limited to the breach of citizens' fundamental human rights. Moreover, the deficient legal framework for the protection and regulation of wiretapping gave rise to inefficient institutional framework for the protection of such rights. Moreover, the use of telephone and the social media in the present century have been abused to the extent that people do not exercise self-caution in the use of telephone and other electronic communication equipment and the social media. A whole of personal information are thereby released by individuals to others using the

[21] J Uba, 'The Legislative Framework For Cybercrime In Nigeria: Current Status, Issues And Recommendations', https://www.mondaq.com/nigeria/terrorism-homeland-security--defence/1136732/the-legislative-framework-for-cybercrime-in-nigeria-current-status-issues-and-recommendations Accessed 16 August 2023.

[22] *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v NIMC* (2021) LPELR 55623 CA.

[23] *Ibid.* J Uba.

[24] Nigerian Data Protection Act 2023, Section 50-53.

telephone and the social media, thereby subjecting such information to the potential risk of compromise, hacking or worst of all is wiretapping which oftentimes are unauthorized.

This article found unfortunately that our courts have not started applying the use of modern technologies in its justice administration. With the advent of science and technology and the new wave of artificial intelligence, the courts need authentication equipment and other relevant technologies say to identify valid electronically generated evidence sought to be tendered before it. Unfortunately, this does not exist in our courts which still dwell on analogue systems. As a result, our courts do not have equipment to distinguish between fake and original evidence. Even with the new innovation of the 2011 evidence Act in section 84, the admissibility of computer generated evidence is still posing some problems to the court and justice system that is the problem of authentication as authentication of computer generated evidence and audio and video evidence generated from the computer can be misleading. There is failure of institutions like Nigerian Communication Commission (NCC), Nigeria Information Technology Development Commission (NITDA) etc in the appropriate regulation of network service providers and enforcement of sanctions against privacy breaches. What is most unfortunate is the fact that often time, those enforcements are politicized. NCC rather than effectively discharge their duties, often are in conflict with service providers and sometimes serve as agents of the government in achieving the nefarious objectives of the government against the privacy rights of citizens.

4. Recommendations

It is recommended that the government and security agencies are advised observe and confirm to the 1999 Constitution of the Federal Republic of Nigeria and decease from carrying out actions that derogates from the Constitution especially as it relates to the breach of privacy rights of citizens by way of wiretapping or any other privacy and data rights infringements.

This work recommends for a review of all legislations on privacy and particularly for the enactment of anti-wiretapping legislation which shall stem the tide of wiretapping and its consequential breach on the rights to private and family life as enshrined in the Constitution. The new legislations which the author propagates, should stipulate stiffer punishment for breach of this rights especially as it relates to wiretapping of telephone communications and some other telecommunications. The work, therefore, recommended the need to enact a comprehensive and explicit data protection law and embark on aggressive awareness campaigns on the rights of citizens to the protection of the privacy of their data.

The authors recommend citizens on self regulation as posited by Irwin Altman in his theory on privacy. People should therefore be mindful of what they write or say through telephone and the social media because of the risk of privacy breach. No wonder Senior Tory of the British Parliament advised parliamentarians to be mindful of the use of phone because of the vulnerability to hacking. Beyond self regulation, laws should be passed requiring telephone companies to report unlawful taps to law enforcement officials as soon as they are discovered, instead of just taking the tap off. Other legislatively imposed surveillances may be desirable, too.

The courts should begin to advance in its use of modern technologies in its justice administration. That will help them to distinguish between true or fabricated electronic evidence and living up to the reality of the prevent day especially with the rising wave of

artificial intelligence. The courts are also called upon to be proactive in protecting the rights of citizens to their privacy by way of judicial activism; awarding damages and appropriate punishments when need be.

The Institutions saddled with the responsibilities of data protection and privacy protection in Nigeria should stand up to their responsibilities in helping to prevent privacy breaches especially as it relates to wiretapping of telephone and some other telecommunications. Again, there should be restrictions to the import, manufacture, and commerce of wiretapping equipment providing for adequate licensing and authorization for its use.