UNAUTHORIZED WIRETAPPING OF PRIVATE TELEPHONE COMMUNICATIONS: APPRAISING THE LEGAL FRAMEWORK FOR THE PROTECTION OF RIGHTS TO PRIVACY IN NIGERIA*

Abstract

The continuous wiretapping of citizen's telephone conversation and some other telecommunications has in the recent times in Nigeria, not only raised serious fundamental rights issues relating to the rights to private and family life but is also plunging the country into a state of anarchy. This has oftentimes necessitated a breach of citizens' fundamental human rights and capable of plunging the nation into a state of lawlessness, if not eradicated or at best curtailed. As part of the aims of the study, this work discussed unauthorized wiretapping of private telephone and some other telecommunications in Nigeria, and appraised the rights to privacy in Nigeria vis-a-vis the need to promote public safety, national security and public interest. This work also discussed the existing legal framework for the use of telephones and telecommunication and the protection of same and its efficacy under the Nigeria and the human rights issues. 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 work found that there is wanton infringement of privacy rights in Nigeria by security agencies, service providers and even individuals. That the Federal government uses top security departments, network service providers and the Nigeria Communications Commissions to wiretap into oppositions party members privacy in order to witch-hunt them. The work also found that there is deficient legal framework for the protection and regulation of wiretapping save the provisions of section 37 of the Constitution which is always abused. The authors therefore recommended for the review of the telecommunication regulations, privacy regulation in Nigeria and security protection laws and guidelines in line with international best practices. The work also recommended for stipulation of strong sanctions for breach of this privacy rights.

Keywords: Unauthorized Wiretapping, Private Telephone Communications, Right to Privacy, Legal Framework, Nigeria

1. Introduction

The advancements in Information and Communications Technology (ICT) have brought this generation to a situation where everything is moving at fast pace.[1] The 20th Century witnessed rapid and new innovative technologies in line with the use of internet, bringing fundamental changes in the way things happen, for instance, the way we live, work and think in this world of digital technology whereby people are peering to the new horizon.[2] The telephone is one of the most important ICT tools for personal communication and for businesses. Telephone has been often seen as a tool to communicate at a distance from one point to another (a one-to-one medium).[3] Although the world's communications systems are advancing dramatically, socially many people have moved from using the telephone to using social media, text messaging and emails, this has partly been because of the high cost of live telephone calls and partly for convenience. However the importance of **telephone systems for** personal communication and **businesses** has remained constant**,** this is due to the limitations of these other communication methods which are unlikely to replace telecommunication for personal and business purposes. Notwithstanding the usefulness, telephone has a number of harmful effects which includes but not limited to stress, anxiety, accident, risk of cancer, cyber bullying, vision problem etc. The use of telephone and other telecommunication, also poses serious challenges to the national security. All phones are a security risk as data communication through telephone is also unsecured and has potential risks of compromise. No wonder a member of the British Parliament, Senior Tory MPs have told The Telegraph that MPs are "constantly" asked to be vigilant to the threat of hacking: "every phone, government or private, can be hacked easily," they said. "Government phones have no extra protection and swapping numbers just means whoever wants to attack your phone has to find the new number and that will take what? 10 minutes? So there shouldn't be any secret information on phones."[4] This article therefore examines to legal framework for the protection of privacy rights in Nigeria especially as it relate to protection against wiretapping of telephone communications.

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

Constitution of the Federal Republic of Nigeria 1999 (as amended)

The Nigerian Constitution being the *grundnorm* from which every other law derives validity and force, recognizes and upholds the fundamental human right of privacy in its Section 37. This section expressly provides to wit: ''the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected'. Although this provision omits the definition of the term privacy and its scope appears to be limited, it can be argued that this provision incorporates both the traditional and modern concept of privacy. This is because section 37 is similar to Article 8 of the European Convention on Human Rights on which Lopez and Babulescu's cases[5] were decided. These cases relate to the modern concept of privacy. The right in Article 8 is, however, subject to certain restrictions imposed by the law and such

***By Ogugua V.C. IKPEZE, PhD**, Professor and Dean, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria, diaikpeze@gmail.com; and

***Chukwunonso Augustus ANIEKWE, LLB, BL, LLM (NAU, Nigeria), PhD Candidate,** Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. Tel: +234 806 6922 005, +44 775 2632 729, Email: justiceaniekwe@gmail.com

[1] A Verma, *Cyber Crimes and Law*, (1st edition, Allahabad, Central Law Publications, 2009), p.3.

[2] B Colin and S Lara, The International Bank for Reconstruction and Development: The World Bank, InforDev and The International Telecommunications Union, (2001), *Telecommunication Regulation Handbook* (10th Anniversary Edn,).

[3] G Balbi, *Studying the Social History of Telecommunications. Between Anglophone and Continental Traditions*. (Media History 15, no. 1 2009) pp. 85–101. doi:10.1080/13688800802583331. See also G Balbi and C Berth, *Towards a telephonic history of technology*, 2019, https://doi.org/10.1080/07341512.2019.1652959, https://www.tandfonline.com/doi/full/10.1080/07341512.2019.1652959, accessed 30 July 2023.

[4] D Sheridan, 'MPs 'constantly' warned their phones are national security risk Liz Truss hacking raises fears of 'insecure' communications at the heart of Government', *Defence Editor* (30 October 2022), https://www.telegraph.co.uk/politics/2022/10/30/mps-constantly-warned-security-risk-liz-trusss-phone-hacked/ accessed 31 July 2023.

[5] *Lopez Ribalda v Spain* (Application No.'s 1874/13 and 8567/13) <https://hudoc.echr.coc.int> accessed on 20 September 2020; and *Barbulescu v Romania* (Application No 61496/08) <https://hudoc.echr.coe.int> accessed on 20 September 2020.

restrictions as are necessary in a democratic society. Thus, Nigeria's data privacy and data protection regime originates from the fundamental legislation of the land. It guarantees citizens the rights to their privacy and the privacy of their homes, correspondence, telephone conversations and telegraphic communication. It is safe to say, therefore, that the rights of Nigerians to data privacy and protection are derived from the Nigerian Constitution. However, beyond the little worded provisions in section 37 of the Constitution, it didn't provide how the rights shall be enforced or protected neither did it provide the punishment for its breach.

Nigerian Data Protection Act 2023 (NDPA)

The Nigerian Data Protection Act, which was recently passed into law by Nigeria's President Bola Ahmed Tinubu, has been acknowledged by stakeholders in the Nigerian Data Privacy Industry to be a novel innovation and a welcome development as it seeks to change the landscape of Data privacy practices in the country. The Act provides a legal framework for the protection of personal information and establishes the Nigeria Data Protection Commission for the regulation of the processing of personal information. The objectives of the Act include: safeguarding the fundamental rights and freedoms and the interests of data subjects as guaranteed under the 1999 Constitution of the Federal Republic of Nigeria; providing for the regulation of processing of personal data; promoting data processing practices that safeguard the security of personal data and privacy of data subjects; ensuring that personal data is processed in a fair, lawful and accountable manner and establishing an impartial, independent, and effective regulatory Commission to superintend over data protection and privacy issues and supervise data controllers and data processors etc. The Data Protection Act introduced salient innovative provisions, as follows: *the establishment of the Nigerian Data Protection Commission (NDPC), introduction of legitimate interests as a basis for processing personal data, provision for data privacy impact assessment, definition of sensitive personal data, and prescription of offences and sanctions for non- compliance amongst others.*

National Security Agencies Act 1986

The National Securities Act of 1986 is an Act that was created to disengage the Nigerian Security Organisation and to create three security agencies, charging each with the conduct of the relevant aspect of the national security and other related matters. These security agencies include: a) The Defence Intelligence Agency, b) The National Intelligence Agency, and c) The State Security Service. The Act expressly provides that these agencies, particularly the NIA and SSS report to the President directly on matters bordering on their functions. This Act has been argued to be 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. This Act therefore needs to be revisited to ensure that its functions and powers do not operate to violate the fundamental rights of Nigerian citizens as it particularly relates to the processing of personal data. Section 1 of the Act provides for the responsibilities of the Defence Intelligence Agency to include but not limited to the prevention and detection of crime of a military nature against the security of Nigeria; the protection and preservation of all military classified matters concerning the security of Nigeria, both within and outside Nigeria; amongst others. While subsection 2 provides for the responsibilities of the National Intelligence Agency, sub section 3 provides for the responsibilities of the State Security Service Unfortunately, subsection 4 of this section of the Act derogates from the Constitution. The section provides that 'the provisions of subsections (I), (2) and (3) of this section shall have effect notwithstanding the provisions of any other law to the contrary, or any matter therein mentioned'.

SSS Instrument No. 1 of 1999

The State Security Service (SSS) is empowered to perform its roles and functions by virtue of SSS Instrument No.1 of 1999 made pursuant to Section 6 of the National Security Agencies[6] (NSA) Act. Worthy of note is the fact that over the years, other decrees (Decree No. 16 of 1976 and Decree 19 of 1986) charged the Agency with identical roles and functions. The SSS as earlier mentioned have highly sophisticated weapons in their arsenal and some of them include; the IMI Tavor Tar-21 assault rifle, FN P90 Personal protection Weapon, FN F2000 assault rifle, some other side arms, and pistols, Improvised Explosive Device detector vans, Mobile IED Jammers for protection of Very important persons in open places, Telephone call interceptors, IMSI number catchers, signal direction finder, armored limousines, etc.[7] The State Security Service is a vital department in the security agency of every country especially Nigeria where security challenges are on the increase. However *in the discharge of its duties, the SSS meddles with the personal data of citizens. The instrument establishing the SSS has become a subject of controversy in that the decree has no regulation whatsoever and is purportedly ranked over Nigeria's Constitution by virtue of its Section 1(4). The Act establishing the SSS also leaves the President with excessive powers to determine the operations of the SSS as the President deems fit. Thus, it is important that they adhere strictly to the provisions of the Constitution and the Nigerian Data It is, therefore, the position of the writer that the National Security Agencies Act be amended to ensure that it guarantees the protection of the rights of data subjects in Nigeria.*

Nigerian Communications Act (NCA) 2003

Section 70 of the Nigerian Communications Act 2003 (NCA 2003) allows the Nigerian Communications Commission NCC to make and publish regulations regarding a variety of subjects, including permits, written authorizations, licenses, offenses, and penalties relating to communication offenses. Using this authority, the NCC issued telecommunications company regulations. Any subscriber whose personal information is stored in the Central Database may request updates under Regulation 9 of the NCC Regulations, in accordance with the rights guaranteed by section 37 of the Constitution, and subject to any guidelines issued by the NCC or a licensee;[8] to have the data kept confidential;[9] not to have subscriber information duplicated except as prescribed by the NCC Regulations or an Act of the National Assembly;[10] and to preserve the integrity

[6] National Securities Act, 1986 Cap. 74, LFN 2004.
[7] W Enang, 'Functions of State Security Service', (2023), https://proguide.ng/functions-of-state-security-service/, accessed 28 September, 2023.
[8] NCC (Registration of Telephone Subscribers), Regulations 9(1)
[9] *Ibid*, Reg. 9(2)
[10] *Ibid*, Reg. 9(3)

of the subscriber's information.[11] The Regulation also requires licensees to utilize subscriber information in accordance with the dictates of the law. Subscriber biometrics may also not be retained after transmission to a central database.[12]The implication of Regulation 10 of the NCC Regulations is that any release of the personal information of a subscriber must be subject to the consent of the subscriber or in accordance with the provisions of the Constitution of the Federal Republic of Nigeria or any other Act of the National Assembly or the NCC Regulations as may be amended from time to time.

Freedom of Information Act 2011

In order to make public records and information more accessible to the public, the FOIA was established. As far as personal records and information and matters concerning personal privacy are concerned, it specifically makes an exception. Unless consent is obtained or the information is publicly available, government agencies are prohibited from disclosing personal information of citizens under section 14 of the Freedom of Information Act.[13]

Economic and Financial Crimes Commission (Establishment) Act 2004

The Economic and Financial Crimes Commission (Establishment) Act (EFCC Act) was enacted in 2002 as the Economic and Financial Crimes Commission (Establishment) Act, 2002; and reenacted in 2004 as the Economic and Financial Crimes Commission (Establishment) Act, 2004. The Act was enacted to combat Economic and financial crimes which were defined under the Act to mean the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration.[14] The EFCC Act creates its own offenses under Sections 14-18, relating to financial malpractices in banks, terrorism, and terrorism financing, false information, retention of proceeds of crime, abetment, and being an accessory to economic and financial crime. More particularly, Section 38 of the Act empowers the officers of the Commission to receive relevant information that is necessary to carry out its functions, protect its informants. The Act also penalizes false information.[15] Governments must not only adopt effective steps to prevent and regulate cybercrime and other offenses utilizing electronic evidence, but they must also do so while respecting human rights and the rule of law.[16]

***National Information Technology Development Agency (NITDA)* Act 2021**

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. The NITDA Regulation prescribes the circumstances under which consent may be extracted.[17] The NITDA Regulation requires individuals engaged in data processing or data control to establish security measures for data protection. These measures encompass defenses against hackers, the implementation of firewalls, the utilization of data encryption technologies, and other similar strategies.[18] NITDA Regulation also provides that data processing by third parties should be governed by written contracts between such third parties and the Data Controller.[19] Violation of the privacy rights of any Data Subject under the NITDA Regulation will result in consequences beyond criminal liability. For Data Controllers managing more than 10,000 Data Subjects, this entails a fine amounting to 2% of the previous year's annual gross revenue or a payment of at least N10 million, whichever sum is higher. In the case of Data Controllers handling fewer than 10,000 Data Subjects, the fine will be 1% of the previous year's annual gross revenue or a payment of ₦2 million, whichever is greater.[20] The NITDA Regulation has established rules which govern the manner in which the provisions of the Regulation should be implemented. The major planks on which implementation rests are discussed below:[21] The establishment of the NITDA Regulation marks a significant and comprehensive effort by Nigeria to formalize the private entitlement to data and its safeguarding. This signifies a level of assurance for both domestic and international stakeholders aiming to invest and engage in business activities within Nigeria, as it demonstrates that the country possesses data regulations comparable to those found globally. This initiative reflects a vital stride in staying up-to-date with the digital revolution and serves as an endorsement of the importance of upholding digital rights within Nigeria. Nigeria's continuous technological advancement is steadily progressing, and the all-encompassing data privacy and protection framework will result in various positive outcomes, outlined in this work.

Police Act 2020

The Police Act of 2020 repeals the Police Act Cap. P19 Laws of the Federation of Nigeria, 2004, and provides for a more effective and well-organized police force. The new Act seeks to make sure that the Police Force following the new law will be driven by the principles of transparency and accountability in its operations and management of its resources. The Act also envisages a police force governed by the fundamental principles of accountability, fairness, justice, and protection of human rights. *In ensuring that the Nigerian Police Force promotes and protects the fundamental human rights of persons guaranteed*

[11] *Ibid*, Reg. 9(4)
[12] *Ibid*, Reg. 9(6)
[13] U V Obi, "Data Privacy and Data Protection Law in Nigeria". https://www.mondaq.com/nigeria/privacy-protection/1183140/data-privacy-and-data-protection-law-in-nigeria Accessed 8 August 2023.
[14] Economic and Financial Crimes Commission Act 2004, Section 46.
[15] Economic and Financial Crimes Commission Act 2004, Section 39(2).
[16]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.
[17] NITDA Regulations, paras 2.3 (1) & (2)
[18] *Ibid*, para 2.6.
[19] *Ibid*, para 2.7.
[20] *Ibid*, para 2.10.
[21] *Ibid*, see para 3.0, 3.1-3.8.

under the Nigerian Constitution, the African Charter on Human and People's Rights, and other international legal charters on human rights, the Police by the provisions of the new Act expected to collaborate with relevant agencies to ensure that the rights of the Nigerian citizen are upheld.[22] *This includes the right to privacy. Also, the Nigerian Data Protection Act provides that the Commission* may file a petition with the Nigerian Police Force on matters relating to the breach of a person's data privacy.[23] It is thus the duty of the Police to ensure that data privacy-related matters are accorded priority and given proper attention, as would any other matter within the scope of their powers and functions.

Terrorism Prevention Act 2022

Amid the challenging landscape of global security, Nigeria has taken a bold step with the introduction of the Terrorism Prevention and Prohibition Act 2022. The Terrorism Prevention and Prohibition Act 2022 provides an effective, unified, and comprehensive legal, regulatory, and institutional framework for the detection, prevention, prohibition, prosecution, and punishment of acts of terrorism, including all forms of terrorism financing, proliferation, and the financing of proliferation of weapons of mass destruction in Nigeria[24]*. The primary objectives of this Act are to establish a solid legal, regulatory, and institutional structure that effectively addresses the complexities of terrorism. It aims to create a united front against this threat by streamlining efforts across different sectors, enabling swift action against those who seek to harm the nation. One crucial aspect of the Terrorism Prevention and Prohibition Act 2022 is its emphasis on adhering to regional and international counter-terrorism conventions and agreements. This demonstrates Nigeria's active participation in the global fight against terrorism and its determination to curb not only acts of terrorism but also the financial support that enables them to thrive. The Act introduces procedures to identify individuals or entities involved in terrorism, thereby enabling the authorities to take decisive action against them. Additionally, the legislation extends the reach of Nigerian courts to hold accountable those involved in terrorism, even if they operate outside the country's borders. At the heart of this legislative effort lies the establishment of committees designed to implement the Act's provisions. These include: (a). The Counter-Terrorism Center, which is a central hub for coordinating policies, strategies, and plans related to counter-terrorism efforts. This center collaborates with various agencies to bolster intelligence sharing and analysis, ensuring a well-coordinated response to the evolving threat of terrorism. (b). The Nigerian Sanctions Committee (NSC) - is entrusted with guiding the designation of individuals or groups involved in terrorism or proliferation. This committee plays a crucial role in aligning Nigeria's efforts with global counter-terrorism initiatives, reinforcing the nation's commitment to international security standards.*

In tandem with the Terrorism Prevention and Prohibition Act 2022, the Money Laundering (Prevention and Prohibition) Act 2022[25] *emerges as an essential ally in the fight against terrorism proliferation. It introduces measures to limit cash transactions and regulate international money transfers, bolstering Nigeria's ability to detect and deter illicit financial activities. However, as our world becomes increasingly digital, one significant gap becomes apparent, namely, the absence of provisions for data privacy. In the age of cyber-terrorism, where digital breaches can lead to grave consequences, it is imperative to have legal frameworks that encompass this crucial aspect of security. To address this evolving threat landscape, the need for comprehensive legislation that covers data privacy becomes even more pressing, ensuring that our nation's security measures stay ahead*

Nigerian Financial Intelligent Unit Act 2018

Nigerian Financial Intelligent Unit (NFIU) Act 2018 was enacted in order to institutionalize best practices in financial intelligence management in Nigeria and strengthen the existing system for combating money laundering and associated predicate offenses.[26] The Act established the Nigerian Financial Intelligence Unit in Section 1(a). It also establishes *a legal framework for a national center responsible for the receipt and analysis of information from financial institutions and designated non-financial institutions for the purpose of generating and disseminating intelligence to all law enforcement agencies and other competent persons in other nations.*[27] *This thus classifies NFIU as a data controller by the definitions of the NDPA. By the provisions of the NFIU Act, the functions of the Unit are multifaceted and largely cut across the receiving, analyzing, and dissemination of information across different agencies within and beyond the country's shores as it relates to financial intelligence and crimes. Being a financial intelligence unit, the NFIU is saddled with some supervisory and monitory functions with the aim of actualizing the objectives of the NFIU Act. Thus, it holds a secure database containing a vast amount of information which includes the personal data of citizens within and outside Nigeria. As is evident from the functions of the Unit, there is a lot of transfer that happens with the information contained in their custody. Due to the independence that the Unit is granted, it is nearly impossible to regulate the operations of the Unit with respect to the handling of citizen's personal data, thereby guaranteeing its protection thereof. As a matter of fact, nothing in the NFIU Act provides for the protection of the personal data of individuals, nor is it in contemplation. This is an obvious pitfall and is essentially not in compliance with the provisions of the Nigerian Constitution as well as the Nigerian Data Protection Act (NDPA).*

Nigeria Communication Commission (Registration of Telephone Subscribers Regulation 2011

Section 9 and 10 of the 2011 Regulation by NCC 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.

[22] Nigerian Police Act, 2020, Section 5 (1-3).
[23] Nigerian Data Protection Act 2023, Section 48.
[24] http://ctc.gov.ng/wp-content/uploads/2022/06/TERRORISM-PREVENTION-publication-6.pdf.
[25] https://www.nfiu.gov.ng/Home/DownloadFile?filePath=C%3A%5CNFIU%5Cwwwroot%5Cdocuments%5CNNQ2_BQPFXB#:~:text=The%20TPPA%202022%20provides%20for,of%20mass%20destruction%20in%20Nigeria, accessed 7 August 2023.
[26] E Jonathan and S C Eze, 'An Examination of the Nigeria Financial Intelligence Unit Act 2018 In the War Against Financial Crimes', https://www.peerreviewedjournal.com.ng/wp-content/uploads/2022/03/AN-EXAMINATION-OF-THE-NIGERIA-FINANCIAL-INTELLIGENCE-UNIT-ACT-2018-IN-THE-WAR-AGAINST-FINANCIAL-CRIMES.pdf Accessed 16 August 2023.
[27] Nigerian Financial Intelligent Unit Act 2018, Section 1 (e).

Cybercrime (Prohibition, Prevention, Etc) Act 2015

Nigeria's Cybercrime Prevention and Punishment Act was established to prohibit, prevent, detect, prosecute, and punish cybercrimes.[28] The Act requires mobile operators, computer and communications service providers to hold subscriber information for a period of two years. The Act therefore stipulates that such service providers are required to protect the confidentiality of the data they process while respecting the individual's right to privacy, as enshrined in the Nigerian Constitution. The Cybercrimes (Prohibition, Prevention, and Punishment) Act of 2015 was passed into law on May 15, 2015. Before this, there was no single regulation in Nigeria that criminalizes cyber or internet-related inactions. As per official sources, the Act sets up a consistent and all-encompassing legal, regulatory, and institutional structure in Nigeria to address the prevention, identification, legal action, and penalties related to cybercrime. Additionally, the legislation safeguards critical national information infrastructure, advances cyber security, and safeguards computer networks, systems, electronic communications, data, software, intellectual property, and privacy rights. The Act further also promotes cyber security and cybercrime prevention by requiring the private sector participant, including ISPs, telecommunication operators, and financial institutions, to report and cooperate with law enforcement agencies such as the Nigerian Police Force and the Nigerian Computer Emergency Response Team (ng-CERT) to enforce Cyber security regulations. The legislation creates a Cybercrime Advisory Council responsible for promoting efficient execution, skill development, engagement with various stakeholders, and collaboration both nationally and internationally. The National Security Adviser takes charge of coordinating Law Enforcement Agencies, while the Attorney General oversees and enhances the legal and institutional structure. According to official sources, the National Security Adviser assumes responsibility for overarching national cyber security efforts. Notable participants include government bodies and private sector enterprises. The Nigerian government is tasked with providing strategic direction in terms of the broader cyber security strategy. The Nigerian Computer Emergency Response Team (ngCERT) was created under the office of the National Security Adviser. Its major objective is to manage the risks of cyber threats in Nigeria's cyberspace and efficiently coordinate incident response and mitigation plans to proactively prevent cyber-attacks against Nigeria. It is situated under the Office of the National Security Adviser.[29] The principal functions of ngCERT includes: to develop a common Situation Awareness platform; to coordinate information sharing on a national scale, to properly handle and coordinate the management of a national-interest incident amongst others. In accordance with Articles 42 and 43 of the Act, The Cybercrime Advisory Council was created in March 2016, with members from a wide variety of ministries and agencies working under the auspices of the National Security Adviser. *Generally, the Cybercrimes Act 2015 has a general impact on cyber law in Nigeria, and its enactment can be said to be the advent of cyber law and protection in Nigeria. It guarantees and provides an effective, unified, and comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. Some of the crimes it provides for include the following:[30] Offences against critical national information infrastructure; hacking Computer Systems and Data Alteration; unauthorized Access of Protected Systems; system Interference; interception of electronic messages, email, electronic money transfers; willful misdirection of electronic messages; unlawful interceptions amongst others.*

Proceed of Crime Act 2022

The primary objective of the Proceeds of Crime (Recovery and Management) Act is to establish a comprehensive framework that addresses the seizure, confiscation, forfeiture, and oversight of properties suspected to have been acquired through illicit activities[31]. This Act covers several critical aspects: The Act encompasses the detection, identification, investigation, and recovery of assets that hold realizable value, including gains and tools employed in unlawful activities managed by relevant organizations. It entails court-issued orders and directives designed to aid in pinpointing, retrieving, and safeguarding the gains and tools associated with illegal activities, as well as properties with realizable worth, overseen by the aforementioned organizations. However, notwithstanding the Act's facilitation of the retrieval and administration of confiscated or forfeited assets, it lacks provisions for safeguarding the data employed in its execution. This omission introduces a vulnerability that affects the Act's adherence to its stipulated provisions including provision on data protection as it relates to telephone communication.

Lawful Interceptions of Communications Regulations 2019

The Nigerian Communications Commission is also charged with regulation of communications in Nigeria[32] and has gone ahead to make a regulation in that regard known as the 'Lawful Interception of Communications Regulations, 2019' (the Regulation), which is an adjunct to the Nigerian Communications Act of 2003.[33] Section 4 of the Regulation[34] provides thus:

> It shall be lawful for any Authorised Agency listed in regulation 12(1) of these Regulations to intercept any Communication or pursuant to any legislation in force, where—
>
> (a) the interception relates to the use of a Communications service provided by a Licensee to persons in Nigeria; or
>
> (b) the interception relates to the use of a Communications Service provided by a Licensee to a person outside Nigeria, provided that the Licensee shall not be liable in any civil or criminal proceedings for damages, including punitive damages, loss, cost or expenditure suffered or to be suffered, either directly or indirectly, for any act or omission done in good faith in the performance of a duty imposed under paragraphs (a) or (b) of this regulation.

[28] *Ibid*, U V Obi
[29] J Uba (n 16).
[30] Cybercrime (Prohibition, Prevention etc) Act 2015, Sections 5-36.
[31] https://placng.org/i/wp-content/uploads/2022/05/Proceeds-of-Crime-Recovery-and-Management-Act-2022.pdf, accessed 15 September 2023.
[32] Section 70 of the Nigerian Communications Act, 2003
[33] Federal Republic of Nigeria Official Gazette, No. 12, 23 January 2019, Vol. 106.
[34] Lawful Interception of Communications Regulations, 2019

In other words, these regulations empower law enforcement agencies to intercept communications provided by communication licensees[35]. 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.
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 shall terminate immediately and further interception shall be treated as unlawful.

The provisions of the Lawful Interceptions of Communications Regulations, 2019 is derogation to the enforcement of the fundamental rights to privacy which may be rooted to section 45 of the 1999 Constitution of the Federal Republic of Nigeria. The 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.

3. Conclusion and Recommendations

It is laudable that Nigerian authorities through their laws and various regulations are taking bold steps to protect the personal data of her citizens. However, despite the array of laws and regulations on data privacy and protection, this dissertation found that there is a wanton infringement of privacy rights in Nigeria by security agencies, service providers and even individuals. Sadly, that the government at all levels uses top security agencies and depart opposition party member's privacy in order to witch hunt them and make cheap political points. There is deficient legal framework for the protection and regulation of wiretapping save the provision of section of 37 of the Constitution of the Federal Republic of Nigeria which is incomprehensive and always abused. There exist some inconsistencies and absurdities in some privacy legislations under review. For instance the newly passed Nigeria Data Protection Act (NDPA) 2023, which introduced 'legitimate interest' as the basis for processing personal data. The Act did not define what amounts to 'legitimate interest' thus giving room for multiple interpretations or misinterpretation. More so, while the NDPA introduced the Date privacy impact assessment to be done by the data controller in order to check the risk of infringement of the rights and freedom of Data subject, the NDPC Commission is yet to establish the mode or regulation for the process as it is empowered to make regulations. These are therefore lacuna that needs to be addressed as soon as possible by the Nigerian legislations. The NSA Act of 1986 unfortunately arrogated absolute powers on itself over the Constitution. The Act state that if any law is inconsistent with the Act, that the Act will prevail. Moreso, the SSS Instrument of 1999 does not only generate controversy as the Decree has no regulations whatsoever, but also section 1 (4) of the Act purportedly ranked over the 1999 Constitution.

The use of telephone (which the authors describe the gadget as a parrot) is vital in the modern day persona communication and business but unfortunately exposes the holder to potential breach of privacy. This is so because once one has a telephone, one's privacy is not guaranteed, anybody can wiretap you at any time without your knowledge. Anybody can wiretap: not just the security agencies and the network service providers but even private individuals. Today, much equipment that can be utilized in wiretapping or eavesdropping may be readily procured by private citizens thereby making the act inevitable. Wiretapping in its nature is unlawful except authorized by law. There is common knowledge therefore amongst the security agencies that wiretapping forms an integral part of their performance of their duties on the guise of national security which often times is not only unauthorised but also abused. Security agencies do not seek recourse to the courts. Ideally the law enforcement ought to seek a court order to wiretap a person only where they have sufficient independent evidence on which they can say that they have reasonable grounds to believe that they will get evidence of crime. Unfortunately, in practice the reverse is the case. They wiretap before anything such that oftentimes, the first time a citizen is aware that he or she has been wiretapped is upon arrest by the law enforcement agencies.

Wiretapping laws are complex and nuanced, with significant implications for human rights and privacy. Interception of communication is an issue that goes to the fundamental right to privacy of individuals as protected under the Constitution of the Federal Republic of Nigeria. It is therefore imperative that the process enshrined in any law or guideline must be unambiguous to ensure there is no room for mischief and to persons gaining nefariously from unauthorized breach of the rights of citizens. Cases and instances of wiretapping abound in the country but none are being punished. This is the reason why

[35]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.

there is lack of case law on the issue of wiretapping in Nigeria. The Nigerian Communications Commission and Security agencies are thus enjoined to swing into action in the punishment of defaulters to set precedence for intending deviants. The government should cease intrusive surveillance and interception of digital communications, ensuring individuals the right to privacy online; and also cease indiscriminate surveillance and monitoring of private telephone conversations, fax transmissions, e-mails, text messages, and internet communications, and ensure that any such surveillance and monitoring is in accordance with the principles of necessity, legitimacy and proportionality. The government should also ensure freedom of expression online by removing restrictions on content and ending censorship measures; and reverse requirements for real-name registration for online users; ensure that safeguards are in place to protect individuals' right to privacy, including by regulating the installation of bugs on telecommunication wires, and others including closed-circuit cameras in private and public spaces and ensuring that the footage from such cameras is strictly protected and not disseminated. This study 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 newly passed Nigeria Data Protection Act 2023 should be reviewed so that the term 'legitimate interest be properly defined and the Nigeria Data Protection Commission should formulate regulations to prevent privacy breaches in the course of impact assessment provided under the Act. 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' 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. It has become imperative to state that the idea of Lawful interception however raises a concern for the potential abuse of privacy rights by law enforcement agencies. Therefore without proper oversight and regulation, wiretapping could be used to target political opponents, intimidate witnesses, or conduct surveillance without cause. Without appropriate checks against abuses, it will pose more dangers by curtailing our liberties than in fighting crimes. Security agencies are therefore urged to desist from flaunting the law in the course of their duties.