ASUU JOURNAL OF HUMANITIES
A Journal of Research and Development
Vol 7, No. 2, April, 2025 pp 279-311

Balancing Communication Surveillance and the Right to Privacy in the Fight against Terrorism in Nigeria.

Nwotite A. & Chinemerem J.C.

Abstract

The impact of terrorism in Nigeria cannot be over-emphasized. The negative affects range from loss of lives and livelihoods, displacements and other humanitarian crises, to economic meltdown being witnessed in the country today. These distasteful effects appeared to have provided the basis for justifying any means, including communication surveillance, employed by security operatives in combating terrorism in Nigeria. However, there is a growing concern over the infringement of the right to privacy by these security operatives. It is against this background that this article examined communication surveillance and the right to privacy, with the purpose of striking a balance between the use of communication surveillance and other electronic correspondence in the fight against terrorism in Nigeria and the right to privacy to communication. To achieve its aim, thearticle adopted doctrinal methodology of legal research, which involves recourse to the primary sources of law such as statutes and case laws; and to secondary sources of law such as relevant textbooks and journals articles. On the basis of the analysis of these materials, the article finds that although there exist a robusts regulatory framework on communication surveillance in Nigeria, the existing framework does not ensure adequate checks for the conduct of communication surveillance in order to forestall the erosion of an individual's right to privacy in the fight against terrorism. To that effect, the article recommended, among others, the introduction of the principle of good faith and bolstering the principle of legality in the framework.

Keywords: Communication Surveillance, Terrorism, Nigeria, Right to Privacy, Security Personnel

Anita Nwotite LLB, BL, LLM, PhD,
Lecturer, Department of Clinical Legal Education,
Nnamdi Azikiwe University, Awka, Anambra State, Nigeria,
am.nwotite@unizik.edu.ng;
+2348039574167

Julius Chukwudi Chinemerem
Student Nigerian Law School,
juliuschukwudi007@yahoo.com ;
+2349050421964

1.0 Introduction

The Nigerian Constitution makes certain guarantees for the enjoyment and protection of every person within the shores of Nigeria. These constitutional guarantees are commonly known and referred to as the fundamental human rights. Among these numerous rights is the right to privacy. Thus, the Constitution stipulates that 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications are hereby guaranteed and protected.' This Constitutional provision is the *fons et origo* of communications/data protection; and communications/data protection laws in Nigeria. In essence, the Constitution, together with other Statutes, drawing validity therefrom, guarantee the inviolability of a person's private communication, including telephone conversations, email correspondences, text messages, WhatsApp, Facebook, X (formerly Twitter) and other social media chats, and all other forms of online and offline communications, in spaces where there is reasonable expectation of privacy.

The right further protects the anonymity of persons who wish to operate anonymously on a public online space. Thus, any conduct which exposes the identity of one who chooses to operate anonymously on a public online space; or which reveals the private correspondences to persons other than those to whom the correspondences were privately directed; will, *prima facie*, be a breach of the right to privacy. However, this article observes that the right to privacy is being breached by intelligent, security and law enforcement personnel in the bid to fight terrorism in Nigeria; and this is justified on the basis of the Constitutional provision in recognition of the need to defend and maintain national security, preserve public order and morality, and for the protection of the rights and freedom of other persons. Thus, the need to monitor, detect and prevent acts of terrorism, and to ultimately maintain security in Nigeria, has given rise to a practice known as communication surveillance, which involves the close observation; or listening to a person's communications (whether online or offline) in the hope of gathering evidence.

An in-depth reporting published by the Institute of Development Studies in collaboration with the African Digital Rights Network in September

of 2023reveals that Nigeria is the African country with the highest spending on surveillance technology, with at least US$2.7 billion spent by the country on known surveillance technology contracts between 2013-2022, excluding the unknown/undisclosed surveillance technology acquisitions by the government. The modes of communication surveillance employed by the Nigerian government on citizens range from internet traffic and mobile data interception, social media monitoring, biometric ID data collection, to the use of smart city/safe city projects in monitoring citizens in open/public spaces.

Ranked as number 8 in the 2024 Global Terrorism Index report produced by the Institute for Economics and Peace, communication surveillance has come to be regarded by some as vital in the fight against terrorism. This explains the enactment of several laws allowing communication surveillance in Nigeria. For instance, the Terrorism Act empowers law enforcement agencies to, among other responsibilities, investigate the acts of terrorism in Nigeria. On the other hand, the Constitution requires that certain acts be done for the purposes of ensuring the security of Nigeria and public interest. Thus, section 45, the Terrorism (Prevention and Prohibition) Act; and other Nigerian laws on communication surveillance, essentially operate as limitations to the right to privacy in Nigeria. Against this background, the article seeks to strike a balance between communication surveillance and the right to privacy in the fight against terrorism in Nigeria.

2.0 Conceptual Framework

The idea of right is to ensure the protection of persons in any given setting. A fundamental right is 'a significant component of liberty, encroachments of which are rigorously tested by courts to ascertain the soundness of purported governmental justifications.' A right is something that is 'due to a person by just claim, legal guarantee, or moral principle.' It includes both legally enforceable rights (fundamental rights); and general human rights (moral and non-justiciable rights). For the purposes of this article, however, a right is seen as a 'legally enforceable claim that another will do or will not do a given act; a recognized and protected interest the violation of which is a wrong.'It describes an enforceable legal claim, to which legal remedy is available upon breach. This definition suggests fundamental right, which has been defined to mean a

right 'derived from natural or fundamental law', the fundamental law being the *grundnorm* – the Constitution.

A right is regarded as guaranteed or protected when it is enshrined in the fundamental law – the Constitution. That being so, rights are enforced as any other provision of the Constitution, and any law that is inconsistent with the provisions of any rights contained in the Constitution will readily be held by the courts to be null and void to the extent of such inconsistency.

The idea of protecting a right is to defend it against infringement through legal guarantees. Thus, protection is intended to 'maintain the status or integrity of a thing, especially through…legal guarantees [and] to shield it from infringement.'

Privacy is one of such protected rights. Privacy is 'the condition or state of being free from public attention to intrusion into or interference with one's acts or decisions.' It is 'the quality of being apart from company or observation; freedom from unauthorized intrusion.'Louis Brandeis simply defined privacy as the 'right to be let alone.'On the other hand, Lucas Introna captured privacy in three (3) senses, to wit: (a) privacy as no access to the person or the personal realm; (b) privacy as control over personal information; and (c) privacy as freedom from judgment or scrutiny by others. Privacy is important as it protects social relationships, intimate relationships, social roles, self-constitution, and autonomy. Privacy, hence, has been recognised as a fundamental human right.

In contrast with the right to privacy, communication surveillance involves the 'close observation or listening of a person or place in the hope of gathering evidence.' It is the 'monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communication networks. In other words, it is an act by which 'third party intercepts a communication in the course of its transmission between intended recipients.' Communication surveillance, thus, involves a coordinated intrusion into a private communication between persons, whether online or offline, by a third party.

Communication surveillance may take the form of wiretapping, internet monitoring, mobile phone interception, fixed line interception, and

intrusion interception. Whatever form communication surveillance takes, it tends to curtail the right to privacy, particularly as enshrined under the Constitution of the Federal Republic of Nigeria. Although communication surveillance has been justified on the basis of national security (lawful), the use of communication surveillance by security personnel in the fight against terrorism in Nigeria has left much to be desired and calls for the balancing of these competing interests.

Terrorism is one challenge facing the world including Nigeria; and its negative effect cannot be overemphasized. In Nigeria, the effort to prevent, prohibit, combat the acts of terrorism and the financing of terrorism; and the implementation of the relevant international treaties and conventions in that regard has seen the enactment of the Terrorism Act. Terrorism has been defined as 'the use or threat of violence to intimate or cause panic especially as a means of affecting political conduct.' The prevalence of terrorism has been buttressed by terrorism insurances taken up by businesses in the bid to mitigate the eventuality of terrorist attacks. Thus, government, through the security agencies, has employed several mechanisms in the fight against terrorism, including resorting to communication surveillance in seeming breach of the right to privacy. In this way, the use of communication surveillance has been justified by the consequences of terrorism.

3.0 Right to Privacy in Nigeria

The Constitution of the Federal Republic of Nigeria guarantees the right to privacy. To that effect, section 37 provides that 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.' The right to privacy allows citizens to safely communicate in the digital space without having any apprehension that their privacy is not protected. It encapsulates the right of a citizen to maintain anonymity, enjoy autonomy, and expect inviolability of his/her information and correspondence over communication networks. Essentially, the right to privacy prohibits any violation or invasion of the privacy of any Nigerian, including the home, correspondence – digital or

otherwise, telephone conversations, and the telegraphic communications of the person.

Apart from the Constitution, other laws in Nigeria also provide for the promotion of the right to privacy. The Nigeria Data Protection Act of 2023 is for instance one of such laws. As part of its objectives, the Act stresses the need to 'safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999.' The Act makes provisions concerning the protection of the data of Nigerians, especially by data controllers and data processors.

Further to that, Nigeria is also a signatory to some international treaties and Conventions protecting the right to privacy. For instance, the International Covenant on Civil and Political Rights to which Nigeria is a signatory provides: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.' The Covenant further guarantees the 'freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.'

Although the right to privacy is notably absent in the African Charter on Human and People's Rights, the African Commission on Human and People's Rights has filled in this *lacuna* by making a soft law extensively protecting the right to privacy through the instrumentality of the Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019.

The Declaration makes elaborate provisions protecting the right to privacy, with specific reference to freedom from interference, confidentiality of communication and personal information, prohibition of indiscriminate communication surveillance.The Declaration also mandates African countries to adopt laws that protect personal information of persons. Suffice it to say that as a constitutionally guaranteed right in Nigeria, the right to privacy cannot be derogated from except in the manner, and to the extent allowed by the Constitution and the other aforementioned laws. Thus, any derogation from the

right to privacy must:

a. be sanctioned by a law that is reasonably justifiable in a democratic society; and

b. for the purposes of maintaining national security, public safety and morality, or for the protection of the rights and freedom of other persons.

4.0 Regulation of Communication Surveillance in Nigeria

In Nigeria, several laws have been passed by the National Assembly permitting communication surveillance, especially for national security reasons.The implication is that communication surveillance laws constitute an exception to the right to privacy as enshrined under the Constitution of the Federal Republic of Nigeria. The communication surveillance laws for instance include: the Cybercrimes Act; the Terrorism Act; and the Nigerian Communications Commission Act (NCC Act), among others. These laws form the legal framework for communication surveillance in Nigeria. The basic objective that cut across these laws is the detection and prevention of crimes and terrorism particularly.

4.1 Nigerian Communications Commission Act (NCC Act)

The Nigerian Communications Commission Act is another such law that allows communication surveillance of persons by the government in Nigeria. The Act mandates service providers to 'upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law in operation in Nigeria and in preservation of national security.' The assistance that may be required of a service provider by a law enforcement agency under this provision of the Act is not defined, hence unrestricted, and could well include the surveillance of communication of persons over the networks of such service provider. The Act, more specifically, empowers the Commission to 'order that any communication or class of communications to or from any licensee, person or the general

public, relating to any specified subject… shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorized officer mentioned in the order.' Law enforcement agencies, in combating terrorism in Nigeria, have this provision as a ready basis for embarking on communication surveillance of individuals in Nigeria.

4.2 Terrorism (Prevention and Prohibition) Act, 2022

Another law permitting communication surveillance in Nigeria is the Terrorism Act, which is the primary law that makes comprehensive provisions to guide the fight against terrorism in Nigeria. Part of its objectives is to provide for 'effective, unified and comprehensive legal, regulatory and institutional framework for the detection, prevention, prohibition, prosecution and punishment of acts of terrorism…in Nigeria,' and further, to provide for 'measures to enable Nigeria to act effectively in the fight against the financing of terrorism.' The Act empowers law enforcement agencies to, with the approval of the National Security Adviser, apply to the Federal High Court, by an ex parte application, for an "Interception of Communication Order" requiring a service provider to intercept and retain communications over its network, and also to enter upon a premises and install communication surveillance gadgets, for the purposes of detecting, preventing or prosecuting acts of terrorism. This provision effectively sanctions both online and offline communication surveillance of individuals by intelligence and security agencies, which act, *prima facie*, constitutes a breach of the constitutionally guaranteed right to privacy. Thus, the Act employs communication surveillance as a method of fighting against terrorism in Nigeria.

4.3 Cybercrimes Act

Cybercrimes Act, was enacted primarily to promote cyber security and protect critical national information infrastructure. The Act also provides for measures that aid the detection and prevention of terrorism through the adoption of communication surveillance mechanisms, thereby limiting the right to privacy. It mandates service providers to retain subscriber information and traffic data and to, at the request of any law enforcement agency, release same to the

requesting agency. Failure by any service provider to comply with such request attracts strict punishment.

4.4 Lawful Interception of Communications Regulations, 2019

Pursuant to the NCC Act, the Nigerian Communications Commission (NCC) also made the Lawful Interception of Communications Regulations, 2019. This Regulation is the most elaborate legal framework for communications surveillance in Nigeria. It provides for the lawful interception of communication; prohibits the unlawful interception of same; provides for judicial oversight of communication surveillance in the form of warrants, spells out the necessary grounds upon which such warrants may be issued; and the duration of same; allows for judicial discretion in the use of information obtained through surveillance as evidence; provides for the mode of complaint; and specifies where the requirement for a warrant may be dispensed with, among other provisions.

5.0 Scope of Communication Surveillance Laws

Communication means the transmission and sharing of information, emotions, attitudes and ideas.On the other hand, communication surveillance can be described as the monitoring and interception of shared information by a third party, without the knowledge or permission of the persons among whom the information are being shared. It is 'a deliberate system of keeping a close watch on the behaviours or activities of persons, groups, organisations and institutions suspected of doing something illegal or capable of causing a breach of security by government's security agencies.' In other words, communication surveillance involves the 'monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communication networks.In this case, 'third party intercepts a communication in the course of its transmission between intended recipients.' The third party referred to above may be a private company on its employees;

or a government agency on citizens. The focus of this article is, however, restricted to communication surveillance by law enforcement personnel, intelligence and other security personnel in the fight against terrorism.

Although, *prima facie*, a breach of the right to privacy, communication surveillance is usually justified by surveillance authorities as necessary for the prevention of crime, protection of the rights of others, and ensuring national security and public safety, in accordance with the provisions of the Constitution of the Federal Republic of Nigeria. This is because in our modern society, technology and digital communication networks are being used in encouraging terrorism by spreading ideologies and acquiring new recruits into terrorists sects worldwide. These justifications, in the light of the threat posed by terrorism and high crime rates in Nigeria, undoubtedly make communication surveillance essential to national security, with some writers describing it as a 'key aspect of modern security.' Other writers have called for the use of 'satellite technology to monitor the activities of insurgents,' and for the deployment of surveillance and communication intercepting technology in the fight against terrorism in Nigeria.

In its bid to prosecute the fight against terrorism, the Nigerian government has enacted several legislations permitting the surveillance of communication of persons within Nigeria, and spent in acquiring a number of communication surveillance technology. The combined effect of these communication surveillance laws and the technology available to the Nigerian government is the mass surveillance of citizens, albeit without due checks, hence, arbitrary. In doing this, the government has employed several modes of communication surveillance ranging from internet traffic and mobile data interception, social media monitoring, biometric ID data collection, to the use of smart city/safe city projects in monitoring citizens in open/public spaces. These involve the interception of private messages and emails sent over internet networks among persons; listening in on mobile phone calls and text message exchanges among persons; monitoring of social media activity and posts of persons, including acquiring the location from where the individual is operating; gathering of the biometric data of individuals through the National Identity Card and Bank Verification Number programmes, and the mandate to link these biometric information to one's sim cards; and the installation of

onsite surveillance equipment in targets' residences and other places.

The use of communication surveillance has recorded laudable successes in the fight against terrorism by the Nigerian government. An instance of this is the recent capture by the Nigerian Army of a Nigerian syndicate supplying fuel to rebels for terrorist activities in Taraba State. The Nigerian Army Headquarters attributed the success of the operation to 'extensive terrorism' and actionable intelligence.

Unfortunately, these surveillance technologies are equally being used for purposes other than combating terrorism and preventing high crimes, and without regard to due process. For instance, in 2019, Nigerian security agencies seized mobile phones, desktop and laptop computers belonging to journalists of Daily Trust Newspaper at their Abuja office, and, without obtaining any warrant, deployed forensic technology that is designed to extract information, including encrypted data, emails, web history, instant messages, social media activities, etc., from phones and computers, for the purpose of identifying a journalist who was reporting on the operations of the Nigerian Military. There have also been reports of the deployment of surveillance technologies in matters that do not concern national security, such as the suppression of activism and for witch-hunting political opposition. Known instances of this are the use of communication surveillance technology by some erstwhile Governors in Nigeria to spy on their opponents. Other instances include the deployment of the technology to identify, trail, and target critics of government officials, agitators, and activists as captured in the report by the Institute of Development Studies. The scope of communication surveillance in Nigeria, therefore, is expansive, indiscriminate, and loosely regulated by law. As shown above, intelligence and security agencies, under the guise of fighting terrorism and maintaining national security have deployed the communication surveillance technologies indiscriminately on Nigerians, and politicians in government are using them on their political opponents. These practices have extensively widened the scope of communication surveillance in Nigeria as envisaged by the laws permitting it.

6.0 Communication Surveillance as an exception to the Right to Privacy

The right to privacy is constitutionally guaranteed. It entails the inviolability of the private correspondence, electronic or otherwise, of citizens by the government or any persons, institutions or bodies whosoever. The right to privacy consists of a number of components - the right to non-interception of electronic communication among persons; the freedom to interact anonymously over the digital environment (including social media networks, internet browsers, electronic mail services, etc.); the guarantee against the monitoring of one's online activities by a third party; to mention but a few. Thus, any act by any person, authority, bodies or institutions inconsistent with this right constitutes a violation of the right of privacy. However, notwithstanding that the right to privacy is a constitutionally protected right, like many other fundamental rights guaranteed by the Constitution, the right is not absolute. The Constitution thus provides for circumstances under which the right to privacy can be derogated from.Hence, by the clear provisions of section 45(1), some fundamental rights, the right to privacy inclusive, may be curtailed. Such circumstance that may occasion the derogation of the right to privacy includes national security, public health or morality, safety and order, and the protection of the rights and freedoms of persons. To that effect, section 45(1) (a) and (b) provides as follows:

> 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 person.

To ensure that this derogation is not arbitrary however, the Constitution also provides for the ambit within which the derogation will be justified. Thus, the derogation must be in pursuance of 'a law that is reasonably justifiable in a democratic society.' The implication is that whether communication surveillance will be lawful or unlawful depends on the following grounds:

a. the purpose for which it was carried out; and

b. whether it is justified by any law.

These grounds conjunctively constitute the test for the lawfulness or otherwise of a communication surveillance in Nigeria.

In pursuance to section 45 of the Constitution several Acts of the National Assembly and other Regulations have been put in place in support of communication surveillance. For instance, the Cybercrimes Act which authorizes the Federal High Court to order a service provider to 'intercept, collect, record, permit or assist competent authorities with the collection or recording of content data and/or traffic data associated with specified communication transmitted by means of communication system.' The Nigerian Communications Commission Act equally limits the right to privacy by empowering the Nigerian communications Commission to 'determine that a licensee or class of licensee shall implement the capability to allow authorized interception of communications…'. Furthermore, the Terrorism Prevention Act, limits the right to privacy by granting the Federal High Court the power to make an order that would require 'a communication service provider to intercept and retain a specified communication, or communications of a specified description received or transmitted, or about to be received or transmitted by that communication service provider, including the call record data or metadata.' Again, the Lawful Interception of Communications Regulations, made by the Nigerian Communications Commission pursuant to the Nigerian Communications Commission Act, also curtails the right to privacy by providing as follows:

> It shall be lawful for any authorized 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 communication service provided by a licensee to persons in Nigeria; or
>
> (b) the interception relates to the use of a communication service

provided by a licensee to a person outside Nigeria.

From the foregoing, it is obvious that although communication surveillance violates individuals' right to privacy, it may nevertheless be lawful where carried out in defence of national security, maintenance of public health or public safety, or the protection of other persons. Therefore, communication surveillance is an exception to the right to privacy, and laws permitting same constitute exceptions to the right to privacy.

These laws notwithstanding, communication surveillance disturbs the enjoyment of the right to privacy. This is well captured by the Court of Justice of the European Union thus: 'any legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental rights guaranteed by Article 7 of the Charter of Fundamental Rights of the European Union [i.e. the right to privacy].'

6.0 Role of Communication Surveillance in the Fight against Terrorism

Since the aftermath of the September 11 2001 terrorists' attack, terrorism has become one of the burning issues across the world. With the on-going Israel-Palestine conflict, acts and threats of terrorism have been on the increase, as terrorists' organisations have globally 'leveraged on the conflict to further their agenda and call for more attacks.' They have also seized the opportunity to recruit and radicalize new members by inciting sentiments on social media. Actual terrorist attacks have also continued to take place internationally, an instance being the several attacks on over 80 commercial vessels linked to Israel by the Houthis terrorists' group.

On the other hand, a substantial part of West Africa and Nigeria, more particularly, are not spared by the menace. With major and minor internationally acclaimed terrorists determined to inflict violence and undermine national security, terrorism has become a topical issue in the Sahel Africa and in Nigeria in particular. Thus, numerous service men and civilians alike have suffered loss of lives and livelihood on account of terrorists' attacks.

Among the numerous atrocities perpetrated by terrorists in Nigeria is the callous kidnap of at least 200 people (mostly women and children) by members of the Boko Haram terrorists' sect. In another incident, two farmers in Borno state were killed by an Improvised Explosive Device (IED) laid by members of the Islamic State of West Africa Province (ISWAP) terrorists' sect. Most recently, the Boko Haram terrorists claimed responsibility for separate suicide bombings that killed at least 18 people and left 19 persons seriously injured at several locations in Northeast Nigeria.

The consequences of terrorism are perilous, costing lives, limbs, and livelihoods. The destruction occasioned by terrorism has been grouped into direct destruction (which includes the destruction of human capital, i.e. killings and human injuries; and physical capital destruction, i.e. the destruction of infrastructures, goods, and alteration of services). Ali noted that the impacts of terrorism include 'loss of human lives, destruction of property and infrastructure, and curtailment of short-term economic activity.'On the other hand, Sandler and Endersobserved that 'terrorist incidents have economic consequences by diverting Foreign Direct Investment (FDI), destroying infrastructure, redirecting public investment funds to security, or limiting trade.'Little wonder then that statistics released by Statistic ashows that from 2007-2019, Nigeria has, by far, suffered the largest ecoomic impact of terrorism in Africa, losing approximately USD 142 billion to terrorism. The second highest loser to terrorism in Africa within the captured period is Libya, which lost almost USD 5 billion to terrorism. This difference between the loss suffered by Nigeria and Libya highlights the stark spate of terrorists' activities in Nigeria.

Apart from the deaths and injuries resulting from acts of terrorism, the humanitarian disaster resulting from terrorists' attacks cannot be overstated. For instance, about 1.9 million persons are reportedly displaced from their homes in Northeast Nigeria as a result of terrorism. Again, Nigeria's food security is also threatened due to the apprehension of violence faced by farmers in Northeast Nigeria.

The indirect consequences of terrorism include fear, anxiety, damage to mental health, higher security expenditure, unemployment rates, increase in social expenditure, reduction in Foreign Direct Investment (FDI), among others).

Given this long list of havoc, caused by terrorists and acts of terrorism in Nigeria, intelligence and security agencies have adopted various terrorism prevention and counter-terrorism measures in the fight against terrorism in Nigeria. Among these measures is communication surveillance.

Communication surveillance has been justified because of its potency in the fight against terrorism. It affords intelligence and security agencies the edge of monitoring the activities of persons and organisations, especially those engaged in acts or financing terrorism. Through the instrumentality of communication surveillance, intelligence and security agencies acquire prior information of planned terrorists' attacks, and detect covert acts and plans aimed at unleashing terror. With this information, they are able to nip acts of terrorism in the bud. Where an act of terrorism had already been carried out, however, communication surveillance has facilitated the apprehension of those directly and indirectly involved in executing the act.

With increased use of the internet to coordinate terrorist attacks, recruit new members; and to radicalize mostly impressionable young persons, the importance of communication surveillance to combating terrorism is invaluable against the background that it aids in the identification and revelation of individuals behind terrorists' acts, revealing the identity of sponsors of terrorism, and in the interception of private communication regarding plots to carry out terrorist attacks. However, a *prima facie* breach of the right to privacy, communication surveillance has proved effective in the war against terrorism.

7.0 Balancing Communication Surveillance and the Right to Privacy

The various laws on communication surveillance in Nigeria discussed above, without a doubt, limit the right to privacy as guaranteed by the constitution and

reinforced by other laws. This limitation, however, is not without justification as earlier stated. There are, hence, competing interests as to the need to protect and promote the individual's right to privacy on the one hand, and the need to maintain national security and combat crime on the other hand. In order to strike a balance between these two valid interests, certain safeguards are required to be adhered to in any communication surveillance law, so that such laws do not extend from merely limiting the right to privacy, to completely eroding the right. Buttressing this point, the Court of Appeal, per Georgewill JCA, stated thus:

> There is an overriding need to observe at all times the rights of citizens to privacy of their communication and any derogation therefrom should be one under due process and adequate legal checks to safeguard the rights of citizens.

Thus, a balanced communication surveillance law must comply with the principles of legality, necessity, legitimacy, and proportionality. These principles may be broken down as follows:

i. The surveillance must not be arbitrary but must be provided for by law;

ii. The surveillance must be for a purpose which is necessary in a democratic society;

iii. The purpose of the surveillance is for national security, public safety, public order, protection of public health or morals, or the protection of the rights of others;

iv. The surveillance must be proportional to the threat or risk being managed.

In addition to the above, any discretion granted to a surveilling authority under a surveillance law must not be unfettered. There must be judicial oversight, due process safeguards, specific limitations as to time, manner, place, and scope of

the surveillance, and transparency on the nature and scope of its use. These principles and safeguards collectively form the internationally accepted standard which a communication surveillance law must conform with in order not to amount to a breach of the right to privacy.

8.0 Verdict on the State of Communication Surveillance Law in Nigeria: Need for Reform

Having considered the extant communication surveillance laws and regulations in Nigeria, and the internationally accepted standard to protect the right to privacy, one must commend, particularly, the LIC Regulations, for mostly complying with internationally accepted standards. This can be seen in its provisions of judicial oversight, time limitation of surveillance, legality requirement, legitimate purpose condition, mode of complaint, etc. Other Nigerian laws on communication surveillance fall short of these standards. However, the LIC Regulations, although mostly compliant, also fall short in certain regards. For instance, it allows for surveillance without a warrant; it disregards the principle of proportionality; it allows for surveillance of encrypted communication; etc. There is, therefore, a need for an amendment of the LIC Regulations, and of other laws on communication surveillance in Nigeria, in order to protect the right to privacy, by bringing them to total compliance with the internationally accepted safeguards as discussed in this article.

9.0 Conclusion

Thus, communication surveillance, as described above, may be lawful or unlawful. It is lawful where it is done pursuant to, and in line with, a law or regulation permitting same. There is no gainsaying that any act or conduct which derogates from any fundamental right guaranteed in the Constitution must be justified by law, otherwise such conduct will be adjudged unlawful.

While it is true that the LIC Regulation, being the primary regulatory framework for communication surveillance in Nigeria, complies with most safeguards for the protection of the right to privacy, it is equally true that an

amendment of same, and indeed other laws on communication surveillance, is necessary for the protection of the rights of Nigerians to privacy. The war against terrorism will be better served if it is prosecuted with citizens not being indiscriminately targeted with surveillance of their protected correspondence. Given the importance of public support to the success of the war against terrorism, illegal surveillance of the populace may have the result of alienating the public from the intelligence and security agencies, thereby reducing the chances of winning the war against terrorism.

With a proper appreciation of the extent of compliance and non-compliance of the communication surveillance framework in Nigeria vis-à-vis the constitutional right to privacy, it is clear that there is still room for improvement that will maximize the ends of communication surveillance laws as identified in this article, and also reassure citizens of the protection of their right to privacy. This is more so as the constitution which provided for this right does not in itself authorize any derogation therefrom or empower same to be done through any other Act, as with some other rights. Limitations on this right, therefore, must be mindfully imposed so as not to be declared unconstitutional and inconsistent with the constitution. Thus, where the principle of necessity and that of legality are in opposition, the lawmakers/regulatory agencies are advised to defer to the principle of legality.

Further, the LIC Rules should be amended to mandate that judges satisfy themselves, in addition to the requirements already established in the rules, that the investigating authority seeking a surveillance warrant are not acting based on a mere profiling of certain sections of the public, and the purpose of the surveillance being nothing other than security purposes, but have a verifiable and compelling fact that makes the surveillance necessary. In other words, the applying investigating authority must show good faith. This is to ensure that the warrant to surveil is not used for political or other purposes. A derogation from a constitutionally guaranteed right of a citizen must be ensured to be for and

overriding public interest and not for a personal advantage to any individual. Finally, the National Assembly is encouraged to adopt the LIC Rules, with the proposed amendments in this article, into an Act to give it prominence and an increased effect so that acts taken under the regulation will not be eroded by any other Act currently in force.

0 Gaps in the Communication Surveillance laws in Nigeria

Having considered the extant communication surveillance laws and Regulations in Nigeria, on the one hand, and internationally best practices for the protection of the right to privacy on the other hand, it is glaring that most of the Nigerian laws on communication surveillance fall short of these acceptable standards. For instance, while the Cybercrimes Act allows for communication surveillance, it barely meets the requirements of the principle of legitimate purpose. The purposes for which communication surveillance may be allowed under the said Act are so wide, especially with the inclusion of investigation or prevention of cybercrime, no matter how trivial, as a purpose. This does not satisfy the purposes permitted under the principle of legitimacy which, at the minimum, recognizes combatting serious crime as a legitimate purpose. Some cybercrimes, such as cyberbullying and cyberstalking, cannot be reasonably said to be so serious as to warrant surveillance. Furthermore, by requiring that due regard be had to the constitutional right to privacy in carrying out communication surveillance, the Act employs the principle of proportionality. The Act also meets the additional requirement of judicial oversight by way of judges' warrants. This is, however, obviated by the power granted to the Attorney-General of the Federation to authorize communication surveillance under international mutual assistance without any obligation to obtain judges' warrants for such activity. Nothing in the Act suggests that the principles of necessity are adhered to as there is no mandate under the Act for authorities to first have recourse to less restrictive measures before engaging in communication surveillance.

The Terrorism Act also falls short of international best practices. However, it does not regard the principles of necessity and proportionality. This is because nothing in the Act shows that regard should be had to a

concerned individual's right to privacy. Although the Act makes provision for judges' warrants, and these accord with the requirement for judicial oversight, there is no requirement to balance the risk being managed against the surveillance measure to be employed.

Again, although the Nigerian Communications Commission Act meets the requirement for legality and legitimacy as it prescribes 'preservation of national security' as a basis for which communication surveillance may be carried out, this notwithstanding, the Act falls short of other international accepted standards. For instance, the principles of necessity and proportionality are not reflected in the Act. Besides, regard is not had to individuals' rights, and there is obvious absence of judicial oversight in the Act.

On the other hand, the Nigerian Data Protection Act does not permit remote communication surveillance in the form of interception or monitoring of communication of individuals. It allows the decryption of encrypted or coded data by law enforcement agencies pursuant to a judge's warrant. Having the preservation of the right to privacy as one of its objectives, the Act incorporates the four cardinal principles of any good communications surveillance law. To that effect, the Act provides:

> A data controller or data processor shall ensure that personal data is —
>
> (a) processed in a fair, lawful and transparent manner;
>
> (b) collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes…

In addition, the Act further requires that data processing be lawful, where the processing is necessary for the purposes of the legitimate interests pursued by the data controller or data processor, or by a third party to whom the data is disclosed, and that such interests in personal data processing shall not be legitimate where they override the fundamental rights, freedoms and the interests of the data subject (the individual). From the foregoing provisions, one can see that the Act entrenches the principles of legality, legitimacy, and, in

part, the principle of proportionality, as it requires any handling of data to be lawful, for legitimate purpose, and in a manner as not to override an individual's fundamental rights. Nonetheless, the principle of necessity that requires the adoption of the least restrictive measure is absent in the Act. It is pertinent to point out that the relevant provisions of the NDP Act considered herein are applicable only to some aspect of communication surveillance – dealing with personal data only. The provisions do not cover the monitoring and interception of communications, hence, it leaves more to be desired.

Turning to the Lawful Interception of Communications (LIC) Regulations, the Regulation is commendable for mostly complying with international best practices. This is made obvious in the provisions of judicial oversight, time limitation of surveillance, legality requirement, legitimate purpose condition, mode of complaint, among others. Nevertheless, the LIC Regulations also fall short of international best practices in certain regards. For instance, it allows for surveillance without a warrant. It also disregards the principle of proportionality; and allows for surveillance of encrypted communication, among other shortcomings. These gaps need to be filled in to ensure the preservation of the right to privacy.

10. Recommendations

With a proper appreciation of the extent of compliance and non-compliance of the communication surveillance framework in Nigeria *vis-à-vis* the constitutional right to privacy, it is clear that there is still room for improvement that will maximize the ends of communication surveillance laws in combating terrorism in Nigeria so as to reassure Nigerians of the protection of their right to privacy. Hence, limitations to the right to privacy must be mindfully imposed so as not to infringe on this right, and where it violates this right, it must be declared unconstitutional and inconsistent with the Constitution. The principles of necessity, legality, proportionality, and legitimacy must be incorporated in any law permitting communication surveillance. These measures, if fully adopted, will guarantee reasonable protection of the right to privacy amidst the fight against terrorism in Nigeria. To address the challenges in the extant communication surveillance laws already examined above the

study recommends as follows:

(1) Section 52 of the Cybercrimes Act should be amended to subject the power granted to the Attorney-General of the Federation to judicial oversight. Again, section 45(3) of the same Act should be amended to limit the purposes for which communication surveillance may be authorized to matters touching on national security and combating high crimes such as terrorism. It is further recommended that the Act be amended to include provisions mandating authorities to employ communication surveillance as a last resort necessary.

(2) It is the further recommendation of this study that section 146 of the National Communication Commission Act (NCC Act) be amended to strip the Nigerian Communications Commission of the power to require communication surveillance of service providers except with a prior warrant granted by a Judge of the Federal High Court. The section should also be amended to mandate that due regard be had to individuals' rights to privacy, such that communication surveillance is not to be employed except where absolutely necessary, and where the risk being prevented or managed outweighs the need to protect the right to privacy at the time.

(3) More so section 2 of the Nigerian Data Protection Act should also be amended to expand the scope of application of the Act to include operations for the interception and monitoring of communications in Nigeria. Section 3(2) of the same Act should also be amended to render the Act applicable to communication surveillance operations carried out by security agencies for national security, combating terrorism, and other legitimate purposes. The Act should also be amended to adhere to the principle of necessity such that the processing of an individual's data, or surveillance of one's communication generally, shall only be carried out when absolutely necessary.

(4) Certain Regulations of the LIC Regulations need to be amended to bring them into consonance with international best practices. For

instance, Regulation 12(3) should be amended to include, in addition to the requirements already established under the Regulations, a requirement that judges satisfy themselves that surveilling authorities seeking a surveillance warrant are acting in good faith, based on verifiable and compelling facts that make the surveillance necessary, and not based on mere profiling of certain sections of the public, or any purpose other than national security. The surveilling authority should among other things show these by specifically deposing to an additional affidavit to be called an "affidavit of good faith" which will accompany their application to the court for a warrant. This additional requirement is to ensure that the warrant sought is not to be used for political or other illegitimate purposes. Furthermore, Regulation 12(4) (b) and (c) of the Regulations, which allow communication surveillance for 48 hours without a prior warrant in cases involving national security and activities of organized crime, should be amended to include a requirement of imminent danger in the opinion of the surveilling authority based on facts available to them in the relevant moment. This amendment is necessary to ensure that judicial oversight is not eroded by the provisions as presently constituted. It is also recommended that Regulation 5 be amended to provide for severe punishment for unlawful interception of communications. Regulation 16 needs also to be amended to extend government agents who engage in unlawful communication surveillance and not just to service providers. It is further recommended that the interpretation clause under Regulation 23 be amended to include a definition for national security and its scope, so that it does not serve as a blanket to cover illegitimate purposes.

(5) Finally, the National Assembly should adopt the LIC Regulations, with the proposed amendments into an Act of the National Assembly to give it more prominence so that acts taken under the Regulation will not be eroded by any other Act currently in force, as Regulations rank below laws in order of precedence. This enactment will further present an

opportunity to make unlawful communication surveillance an offence attracting severe punishment, as only laws or Regulations creating offences and prescribing punishments for same can prohibit an act or omission in Nigeria

References

Constitution of the Federal Republic of Nigeria, 1999 (as amended) (CFRN).
CFRN, section 37.
CFRN, section 37.
For example, the Nigeria Data Protection Act of 2023 (NDPA), and the Nigerian Communications Commission Act, 2003.
Sec. 24(1)(f) & (2) NDPA
Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019 (DPFEAIA), Principle 40(2).
CFRN, (above note 3), 37; NDPA sections. 24(1)-(3) & 46(1); DPFEAIA, Principle 40.
CFRN, (above note 3), section 37.
BA Garner, *Black's Law Dictionary* (9th edn, USA, Thompson Reuters 2009), 1583.
Institute of Development Studies, Press Release: 'Nigeria Spending Billions of Dollars on Harmful Surveillance of Citizens' (27 September 2023) <https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/> Accessed 16 June 2024.
Roberts T., *et al*, 'Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia' (2023) *Institute of Development Studies*, 5 <https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/18120/ADRN_Surveillance_Supply_Chain_Report.pdf?sequence=26&isAllowed=y> Accessed 9 July 2024.
Ibid, 48-55.
Institute for Economics and Peace, 'Global Terrorism Index 2024' (2024) *Institute for Economics and Peace*, 6 <https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf> Accessed 16 June 2024.
T Ilori'Framing a Human Rights Approach to Communication Surveillance Laws Through the African Human Rights System in Nigeria, South Africa and Uganda' *African Human Rights Yearbook* [2021] 5 (8), 136.
Terrorism (Prevention)(Amendment) Act, 2013, section 2(5)(a)-(i).
CFRN, section 45.
CFRN.
2022.
Bryan A. Garner, 744.
*Ibid*1436.
The scope of this article is limited to rights in this sense.
E.g CFRN, Chapter II; AONwafor, 'Enforcing Fundamental Rights in Nigerian Courts – Processes and Challenges', [2009] (4) *African Journal of Legal Studies*,

2.
Ibid.
BA Garner, 744.
Ibid.
AO Nwafor, 3.
Ibid.
CFRN, section 1(3).
CFRN,section 1(3).
<merriam-webster.com/dictionary/protect> accessed July 5, 2024.
CFRN, (above note 3), section 37.
Bryan A. Garner (above note 12), 1315.
<https://merriam-webster.com/dictionary/privacy> accessed July 5, 2024.
On the SCOTUS 1916-1939
Dissenting opinion in *Olmstead. v United States* (1928) 277 U.S. 438 at 478.
Lucas D. Introna, 'Privacy and the Computer: Why We Need Privacy in the Information Society' [1997] (28) (3) *Metaphilosophy*, 261-262.
Ibid, 265.
CFRN, section 37.
BA Garner (above note 12), 1583.
Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2013) A/HRC/23/40, UN Human Rights Council, para 6 <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> accessed 5 July 2024.
Privacy International, 'Communications Surveillance: Distinctions and Definitions', *Privacy International* (2018) <www.privacyinternational.org/course-section/2088/communications-surveillance-distinctions-and-definitions> accessed 5 July 2024.
Privacy International, 'Communications Surveillance', *Privacy International* (2018) https://privacyinternational.org/explainer/1309/communications-surveillance> Accessed 5 July 2024.
TIlori, 138.
Terrorism (Prevention)(Amendment) Act, 2013.
BA Garner, 1611.
Insurance Information Institute, 'Understanding Terrorism Insurance', Insurance Information Institute <https://www.iii.org/article/understanding-terrorism-insurance> Accessed 6 June 2024.
CFRN, section 37.
T Ilori, 136.
CFRN, section 37.
CFRN.
CFRN, section 37; NDPA, Sec. 25(2)(c)
Ibid.
Nigeria Data Protection Act, 2023 (NDPA).
NDPA, section 1(a).
Ibid.

Ibid, section 29.
International Covenant on Civil and Political Rights International Covenant on Civil and Political Rights, 1966 (ICCPR).
ICCPR, Art. 17(1).
Ibid, Art. 19(2).
Principles 38 and 42.
DPFEAIA, Principle 38.
DPFEAIA, Principle 40.
Ibid, Principle 41.
Ibid, Principle 42.
CFRN (above note 3), 45(1).
Ibid.
Ibid, section 37.
Examples include the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015; Terrorism (Prevention and Prohibition) Act, 2022; Lawful Interception of Communications Regulations, 2019, made pursuant to the Nigerian Communications Commission Act, 2003; to mention but a few.
Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, sections 38 & 39.
Terrorism (Prevention and Prohibition) Act, 2022, section 68.
Nigerian Communications Commission Act (NCC Act), 2003, 146-148.
NCC Act.
Ibid, section146(2).
NCC Act, 148(1).
Terrorism (Prevention and Prohibition) Act, 2022.
Ibid, section 1(a).
*Ibid,*sec. 1(f).
Terrorism (Prevention and Prohibition) Act, section68(1) & (2).
Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
Ibid, section 1.
Ibid, section 38.
Cybercrimes (Prohibition, Prevention, etc.) Act, section 38(1)-(3).
Ibid,section 38(6).
Ibid, section 70.
Lawful Interception of Communications Regulations, 2019, Regulation 4.
Ibid, Regulation 5.
Ibid, 7(1).
LIC Regulations, Regulation 7(2) & (3).
Ibid, Regulation 14(1).
Ibid, Regulation 17.
Ibid, Regulation 20.
Ibid, Regulation 8 & 12(4).
Akpama E., 'Counselling for Effective Communication: A Tool for National Security' [2013] (4) (7) *Journal of Education and Practice*, 31-36, 31 <https://iiste.org/Journals/index.php/JEP/article/download/5269/5278> accessed 13 July 2024
A.I. Oludare, *et al*., 'The Use of ICT Tools in Tackling Insecurity and Terrorism Problem in Nigeria' [2015] (5) (5) *Network and Complex Systems*, 32

<https://www.iiste.org/Journals/index.php/NCS/article/download/22824/22722> accessed 13 July 2024

Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2013) A/HRC/23/40, UN Human Rights Council, para 6 <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> accessed 15 June 2024.

Privacy International, 'Communications Surveillance: Distinctions and Definitions' (2018) <www.privacyinternational.org/course-section/2088/communications-surveillance-distinctions-and-definitions> accessed 15 June 2024.

Scott A. Faust, et al., 'Employee Monitoring and Surveillance', *Reuters* (1 May 2023) <https://www.reuters.com/practical-law-the-journal/transactional/employee-monitoring-surveillance-2023-05-01/> accessed 13 July 2024

T Ilori, 136

CFRN, section 37.

T Ilori, 136.

Section 45(1).

Archetti C., 'Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age' [2015] (9) (1) *Perspectives on Terrorism*, 49 <https://www.jstor.org/stable/26297326> accessed 13 July 2024.

LatifatOdeniyi and Haruna Abdullahi, 'Information Communication Technology and Terrorism in Nigeria: Digitalization for Enhanced National Security' [2022] (3) (1) *International Journal of Information Systems and Informatics*, 17 <https://journal.jis-institute.org/index.php/ijisi/article/download/669/466> accessed 13 July 2024

A.I. Oludare, *et al*., 21-22.

Ibid, 32

The following are examples of laws permitting communication surveillance by the government in Nigeria: Cybercrimes (Prohibition, Prevention, etc.) Act, 2015; Terrorism (Prevention and Prohibition) Act, 2022;Nigerian Communications Commission Act, 2003; Lawful Interception of Communications Regulations, 2019, made pursuant to the Nigerian Communications Commission Act, 2003.

Institute of Development Studies, Press Release: 'Nigeria Spending Billions of Dollars on Harmful Surveillance of Citizens' (27 September 2023) <https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/> Accessed 16 June 2024.

Victoria Ibezim-Ohaeri, et al., 'Security Playbook of Digital Authoritarianism in Nigeria' (December 2021) *Action Group on Free Civic Space*, 46 <https://closingspaces.org/download/7808/> accessed 13 July 2024

Roberts T., *et al*., 48-55

Justice Okamgba, 'SIM-NIN Linkage: NCC Rules Out Extension, Telcos Bar 12 Million Lines', Punch News (Abuja, 29 February, 2024) <https://punchng.com/sim-nin-linkage-ncc-rules-out-extension-telcos-bar-12-

million-lines/> Accessed 10 July 2024.

Terrorism (Prevention and Prohibition) Act, 2022, Sec. 68(2)(b).

Nigerian Army Headquarters, Official Statement on X: 'Troops Apprehend Nigerian Syndicate Supplying Fuel to Ambazonia Rebels for Terrorism Activities in Taraba State' (24 May 2024) <https://x.com/HQNigerianArmy/status/1794050267698127348?t=5syU-Ffgz8lqXbKhuAauLQ&s=08>

Nigerian Army Headquarters (above note 155).

AbdulkareemMojeed, 'Nigerian Military Using Surveillance Technology to Spy on Nigerians – CPJ', *Premium Times* (Abuja, 28 October 2019) <https://www.premiumtimesng.com/news/top-news/359898-nigerian-military-using-surveillance-technology-to-spy-on-nigerians-cpj.html?tztc=1> Accessed 10 July 2024

Roberts T., et al (above note 14) 59 & 61

Ogala Emmanuel, 'INVESTIGATION: How Governors Dickson, Okowa Spend Billions on High Tech Spying on Opponents, Others' Premium Times (9 June 2016) <https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html> Accessed 10 July 2024.

Roberts T., *et al*, 61.

International Commission of Jurists, 'Report on Regulation of Communication Surveillance and Access to Internet in Africa' *International Commission of Jurists* (2021) 35 <https://www.kas.de/documents/275350/0/Report-on-Regulation-of-Communications-Surveillance-and-Access-to-Internet-in-Selected-African-States.pdf/> accessed 10 July 2024.

CFRN, section 37.

ICCPR, Art. 17.

Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2013) A/HRC/23/40, UN Human Rights Council, para 6 <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> accessed 15 June 2024.

Article 19, Policy Brief: 'Right to Online Anonymity', Article 19,6 (June 2015) <https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf> accessed 17 July 2024.

DPFEAIA, Principle 39(2).

CFRN, section 37.

Ibid.

Ibid.

Ibid.

Ibid.

CFRN 1999.

Ibid, section 45(1)(a)&(b).

CFRN, section 45(1)(a)&(b).

Ibid.

Ibid, section 45(1).
Ibid, section 45(1)(a)&(b).
Ibid, section 45(1).
Cybercrime (Prohibition, Prevention, etc.) Act 2022, section 39(a).
Ibid.
Nigerian Communications Commission Act 2003, section 147.
Ibid.
Terrorism (Prevention and Prohibition) Act 2022, section 68(2)(a).
Ibid.
Lawful Interception of Communications Regulations 2019, regulation 4(a)&(b).
Nigerian Communications Commission Act 2003, section 70.
Lawful Interception of Communications Regulations 2019, regulation 4(a)&(b).
CFRN (above note 3), section 45(1)(a)&(b).
MaximilanSchrems v Data Protection Commissioner CJEU, C-362/14 (2015), para. 94.
Supra.
Supra, para 94.
Since the September 11, 2001 attacks by the Al-Qaeda terrorists on the Twin Towers in New York, USA, terrorism has remained a source of worry to governments and the people across the globe, with all hoping and fighting against the reoccurrence of such tragedy ever again.
Fabian Koh, 'Terrorism Threat Elevated since Renewed Israel-Palestine Conflict; Singapore Also Affected: ISD', *CNA* (Singapore, 25 July 2024) <https://www.channelnewsasia.com/singapore/terrorism-threat-elevated-renewed-israel-palestine-conflict-singapore-also-affected-isd-4503686> Accessed 25 July 2024.
Ibid.
Ibid.
Ibid.
Aljazeera, 'Over 1,800 'terrorist attacks' in West Africa in 2023: ECOWAS', *Aljazeera* (West Africa, 26 July 2023) <https://www.aljazeera.com/news/2023/7/26/over-1800-terrorist-attacks-in-west-africa-in-2023-ecowas> Accessed 16 June 2024.
Ibid.
Chinedu Asadu, 'At Least 200 People, Mostly Women and Children, Abducted by Extremists in Northeastern Nigeria' *AP News* (Abuja, 7 March, 2024) <https://apnews.com/article/nigeria-borno-gamboru-ngala-un-kidnap-b3290a225d78951b0a7acdb5642f2453> Accessed 24 July 2024.
Sahara Reporters, 'Two Nigerian Farmers Killed in Fresh Bomb Explosion on Borno Road', *Sahara Reporters* (30 June 2024) <https://saharareporters.com/2024/06/30/two-nigerian-farmers-killed-fresh-bomb-explosion-borno-road> Accessed 24 July 2024.
29th June, 2024.
News Wires, 'Multiple Suicide Bombings Kill at least 18 People in Northeast Nigeria', *France24* (30 June, 2024).
Arshad Ali, 'Economic Cost of Terrorism: A Case Study of Pakistan' [2010] (30)

Institute of Strategic Studies Islambad, 1 <https://www.issi.org.pk/wp-content/uploads/2014/06/1299569657_66503137.pdf> Accessed 26 July 2024.

Todd Sandler and Walter Enders, 'Economic Consequences of Terrorism in Developed and Developing Countries: An Overview', in P. Keefer and N. Loayza (eds.), *Terrorism, Economic Development, and Political Openness* (Cambridge: Cambridge University Press, 2008) 17-47, 17 <https://dx.doi.org/10.1017/CBO9780511754388.002> Accessed 26 July 2024.

Ibid.

Statistica, 'Economic Impact of Terrorism in African Countries Between 2007-2019', Statistica (30 January 2024) <https://www.statista.com/statistics/1197888/economic-impact-of-terrorism-in-africa/> Accessed 25 July 2024.

Ibid.

Ibid.

Umejiaku Nneka Obiamaka, 'Terrorism and Protection of the Rights of Internally Displaced Children in Nigeria: A Legal Appraisal' [2023] (14) (2) *NAUJILJ*, 80 <https://www.ajol.info/index.php/naujilj/article/view/257390/243123> Accessed 25 July 2024.

BudgIT Foundation, 'Nigeria's Rising Insecurity: Implications for the Nigerian Economy' *BudgIT* (15 April 2024) <https://budgit.org/nigerias-rising-insecurity-implications-for-the-nigerian-economy/> Accessed 25 July 2024.

O. B. Alade, et al, 'Terrorism, Human Capital Development and Economic Growth in Nigeria' [2021] (2) (2) *IJEDR*, 142 .

Anas Shehu, et al, 'Remote Surveillance: A Means of Intelligence Gathering for Minimizing Security Challenges in Nigeria' [2022] (XXIX) (4) *Journal of Engineering Science*, 68

NATO, 'Joint Intelligence, Surveillance and Reconnaissance' *NATO* (7 March 2024) <https://www.nato.int/cps/en/natolive/topics_111830.htm> Accessed 16 June 2024.

Kevin D. Haggerty and Amber Gazso, 'Seeing Beyond the Ruins: Surveillance as a Response to Terrorists Threats' [2005] (30) (2) *Canadian Journal of Sociology*, 181 <https://www.jstor.org/stable/4146129> Accessed 26 July 2024.

The Jakarta Post, 'Police Track Foreign Funding of IS-Linked JAD', *The Jakarta Post* (Jakarta, 26 July 2019) <https://www.thejakartapost.com/news/2019/07/26/police-track-foreign-funding-of-is-linked-jad.html> Accessed 26 July 2024.

Kevin D. Haggerty and Amber Gazso, (above note 24).

Ibid.

Ibid.

Terrorism (Prohibition, Prevention, etc.) Act, Section 1(a) thereof, which specifically provides for the objectives of the Act to include the detection, prevention, and prosecution of acts of terrorism in Nigeria.

Fabian Koh, 'Terrorism Threat Elevated since Renewed Israel-Palestine Conflict; Singapore Also Affected: ISD', *CNA* (Singapore, 25 July 2024) <https://www.channelnewsasia.com/singapore/terrorism-threat-elevated-renewed-israel-palestine-conflict-singapore-also-affected-isd-4503686>

Accessed 25 July 2024.
Ibid.
Ibid.
Branislav Todorovic and Darko Trifunovic, 'Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes', in Alex P. Schmid (ed.), *Handbook of Terrorism Prevention and Preparedness* (The Hague; ICCT Press Publication, 2021) 604 <https://www.icct.nl/sites/default/files/2023-01/Chapter-19-Handbook.pdf> Accessed 26 July 2024.
The Jakarta Post, 'Police Track Foreign Funding of IS-Linked JAD', *The Jakarta Post* (Jakarta, 26 July 2019) <https://www.thejakartapost.com/news/2019/07/26/police-track-foreign-funding-of-is-linked-jad.html> Accessed 26 July 2024.
Anas Shehu, 63
Section 37, CFRN 1999
Paradigm Initiative &Ors v Attorney General of the Federation &Ors (CA/L/556/2017)
T Ilori, 140.
Ibid.
Frank La Rue, para. 29.
T Ilori (above note 17),141.
Regulations 7,12,13&14, LIC Regulations
Regulations 13(1)(e) & 14(1), LIC Regulations
Regulation 5, LIC Regulations
Regulation 7(3), LIC Regulations
Regulation 20, LIC Regulations
Regulation 12(4), LIC Regulations
Regulation 9, LIC Regulations
T Ilori, 138.
CFRN, section 45(1).
For instance, the constitution provides for exceptions to the right to life – sec. 33(2); right to dignity of human person – sec. 34(2). The constitution also empowers some rights to be limited by any other law, e.g. the right to personal liberty – sec. 35(7)(b); right to freedom of expression and the press – s.39(2)&(3).
CFRN, section 1(3).
Adherence to the principles of legality, legitimacy, proportionality and necessity in the conduct of communication surveillance.
Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
Ibid, section 38 and 39.
Ibid, section 38(4) and 45(3).
Ibid, section 45(3).
SpaceNet and Telekom Deutschland, Supra.
Cybercrimes Act, section 38(5).
Ibid, section 39 and 45.
Ibid, section 52.
Terrorism (Prevention and Prohibition) Act, 2022, section 68.
Ibid, section 68(1).

Terrorism (Prevention and Prohibition) Act, section 68.
Nigerian Communications Commission Act, 2003.
Ibid, section 146(2).
Nigeria Data Protection Act, 2023.
Ibid, section 58(3)(f).
Ibid, section 1(1)(a).
Ibid, section 3(2)(a) – (c).
Ibid, section 24(1)(a) – (c).
Ibid, section 25(1)(b)(v).
Ibid, section 25(2)(a).
Nigerian Communications Commission Act, section 2(1).
Lawful Interception of Communications Regulations, Regulations 7,12,13 and 14.
Ibid, Regulations 13(1)(e) & 14(1).
Ibid, Regulation 5.
Ibid, Regulation 7(3).
Ibid, Regulation 20.
Ibid, Regulation 12(4).
Ibid, Regulation 9.
CFRN, section 1(3).
TomiwaIlori, 140.
Particularly where it will infringe on the right to privacy.
CFRN, section 45.
CFRN, section 45.