RIGHT TO PRIVACY AND NATIONAL SECURITY IN NIGERIA: IN SEARCH OF EXACT CONFINES OF ITS BOUNDARY

Written By ***Ibrahim Mohammed*, Kazeem A. Oyinwola**, Dauda U. Dewan******

**LL. B, BL, LLM., Deputy Director (Academics), Nigeria Law School, Kano, Campus, Kano State, Nigeria*

***LL. B(Ilorin), BL(Yola), LLM (Keffi). Managing Partner, Amofin Solicitors, Nigeria. Barrister and Solicitors of the Supreme Court of Nigeria*

****LL M, BL., Senior Lecturer, Nigerian Law School, Kano Campus, Kano State, Nigeria*

ABSTRACT

This paper examined right to privacy and its limitation by the state on ground of national security using Nigeria as case study. Activities of states and non-state actors in relation to right to privacy were critically evaluated. The 'Permissible Limitation Test' developed over time by courts and human rights bodies was also examined. Relying on Articles 26 and 27 of Vienna Convention on Law of Treaties, it was submitted that action(s) which violate right to privacy by state authorities should, in each circumstance, be subjected to the 'permissible Limitation Test'. Furthermore, it was argued that by virtue of the Vienna Convention and the preamble to the Fundamental Rights (Enforcement Procedure) Rules, 2009, Nigerian courts should apply the test in deserving circumstances. It was recommended among others that the UN Human Rights Council should issue a new general comment on right to privacy to provide guidance for states in law enforcement and the courts in Nigeria should ensure derogation from the right to privacy occurs only in deserving cases.

INTRODUCTION

Privacy is a constituent element in the autonomy of an individual and a keystone of a truly modern democracy. Its significance accentuates not only the value it protects but also its recognition and guarantee as a fundamental right in many notable international and regional

human rights instruments including constitutions of many countries in the world.[i] Right to privacy as a fundamental right imposes a negative obligation on the state and non-state authority for its protection. Nevertheless, the various laws guaranteeing right to privacy also make provisions for instances when the right can be derogated from. In order words, the laws also provide permissible limitations to the right to privacy which can be invoked in deserving circumstances to limit the extent of its application.

The permissible limitations to right to privacy provided by law is not the actual challenge because like every other right, right to privacy is not absolute. The challenge, however, is that the permissible limitation is sometimes nebulous, ambiguous or omnibus and can give room for potential abuse by state authorities. For instance, the provisions of section 45 of the 1999 Constitution of the Federal Republic of Nigeria (as amended) have been seen as providing restriction or derogation from fundamental rights generally including right to privacy. The effect of this provision is that right to privacy can be curtailed or even derogated from in the interest of defence, public safety, public order, public morality, public health; or for the purpose of protecting the rights and freedom of other persons.[ii]

These nebulous provisions that limit to right to privacy have consistently been used and relied upon, most times, by state authorities to suppose that once national security is threatened, protection of right to privacy is an inconvenience, and the states must be allowed to do everything possible to avert the threat even if it interferes with individual right to privacy. With little or no legal guidance as regards what constitutes interest of defence or public safety or national security - which is incapable of an exhaustive list - state authorities oftentimes find hiding a place under the omnibus shade of national security to interfere with and violate individual right to privacy with little or no regard to the provision of law.

Although, human rights courts and treaty bodies over time have developed a test, -permissible limitation test- into which a measure or action limiting a fundamental right should be subjected. The UN HRC is yet to issue a General Comment to specifically address the concerns about right to privacy vis-à-vis its limitation by states authorities on the ground of amorphous "national security". Meanwhile, in the absence of a precise legal guidance or effective framework under which state authorities can be challenged or held accountable for violation of

right to privacy, individual right to privacy will become eroded in this age of internet with or no regard to law.

RIGHT TO PRIVACY UNDER THE LAW

Right to privacy is an inalienable fundamental right. It is guaranteed under articles 12 and 17 of the Universal Declaration of Human Rights (UDHR)[iii] and International Covenant on Civil and Political Rights (ICCPR).[iv] These two provisions guarantee the right to privacy and prohibit any form of interference with the right by state including the non-state actors except such interference is in accordance with the law. Regional instruments such as European Convention on Human Rights (ECHR)[v] and the Charter of the Fundamental Rights of the European Union,[vi] American Convention on Human Right[vii] and African Charter on the Right and Welfare of the Child[viii] all have provisions protecting the right to privacy.

In Nigeria, the right to privacy of citizens, their homes, correspondence, telephone conversion and telegraphic information is guaranteed and protected under section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended).

Like the majority of other fundamental rights, right to privacy is not absolute. Each of the human rights instruments guaranteeing it provide instances when it will be lawful to derogate from it. Although at the international level, both articles 12 and 17 of the UDHR and ICCPR respectively do not specifically spell out particular exceptions or limitations to right to privacy. However, articles 29 and 30 of UDHR and articles 41 and 51 of the ICCPR provide instances when right to privacy guaranteed under both instruments can be limited. Article 8(2) of ECHR prohibits specifically any form of interference, by a public authority, with the exercise of right to privacy guaranteed in article 8(1) except in accordance with the law. In addition, such interference must such that it is 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country; for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

Furthermore, the text of Article 7 of the EU Charter provides no specific exception to right to privacy in the Charter, Article 8(1) of the Charter subjects the fundamental right to data

protection guaranteed under it to control by an independent authority. Meanwhile, article 52(1), (2) and (3) of the Charter provide comprehensive claw-back clauses to the rights guaranteed in the Charter. While Article 30 of the ACHR provides the scope of limitation to its right to privacy and other rights guaranteed under it, article 8(2) of ECHR provides specific exceptions to right to privacy guarantee under article 8(1) of the Charter.

At the national level, in Nigerian section 45(1) CFRN provides grounds whereupon the right to privacy guaranteed under section 37 CFRN can be derogated from, limited or circumscribed. The various aforementioned claw-back clauses providing grounds upon which right to privacy can be limited or derogated from are similar save for some slight differences. The areas of similarities with respect to the grounds on which right to privacy can be limited or derogated from include 'the interest of defence', 'public safety'[ix], 'public order', 'public morality' or 'public health', 'sovereignty and integrity of the state'[x], 'friendly relations'[xi], 'economic wellbeing of the country'[xii], or 'for the purpose of protecting the rights and freedom of other persons'[xiii]. Section 45 of the 1999 Constitution of the Federal Republic Nigeria provides to the effect that the provision of section 37 can be derogated from in the interest of defence, public safety, public morality and public and for the protection of the rights and freedom of others. To this effect, state authority can find a hiding place in any of the omnibus provisions allowing derogation from right to privacy to interfere with the right either through its actions, policies or regulations or even through the instrumentality of the law.[xiv]

States have consistently asserted their legitimate right to maintain law and order. In this regards, protection of right to privacy is perceived as an inconvenience once national security is threatened. To this end, states have consistently maintained that they should be allowed to do everything possible to avert an actual or perceived threat to national security even of the measure requires interferes with or invade individual right to privacy.[xv] As legitimate as concern over national security sounds, a number of events have proved that the terms has been invoked in most instances to target individual and violate right to privacy arbitrarily. A few events chronicled below contain such instances.

RIGHT TO PRIVACY AND NATIONAL SECURITY: ACTIVITIES OF STATE INTERFERING WITH RIGHT TO PRIVACY

Notwithstanding the multitude of the provisions of laws guaranteeing right to privacy in many nations around the world, internet users are still being monitored as regards the sites they visit and with whom they are communicating. In some case, states hide under the amorphous provision allowing derogation from right to privacy in the interest of defence or national security. Countries such as Germany, Colombia, United States, Uganda and Bangladesh have been allegedly fingered among countries that illegally spy on citizens, especially journalists, using communications surveillance including placing spies in newsrooms.[xvi] States like Australia[xvii] and Canada have also been alleged to be processing millions of transactions each year through advanced data-mining tools with little regard to individual right to privacy.[xviii]

In fact, according to Privacy International, the Administrative Department of Security of Colombia was found in 2009 to have been conducting illegal surveillance on members of the media, human rights workers, government officials and judges, and their families for seven good years.[xix] This surveillance power was probably taken too far in Greece when unknown third parties set up communication interception by which the communications of Prime Minister of Greece, and dozens of other high-ranking dignitaries were intercepted and listened to.[xx]

In 2007, Bangladesh required third parties offering communication service to turn over records of their users' identities, passwords and personal details to the Bangladesh authorities. After the collection of the record, the authorities visited some users and thoroughly searched their computers and contact lists.[xxi]

The UK has proposed that telecommunications companies should actively monitor and retain information on individuals' online activities including social-networking activities.[xxii] Furthermore, in 2002, the Uganda Anti-Terrorism Act allows wiretapping and searches of the media upon suspicions justifying it.[xxiii] Meanwhile, the US Government's policy on access to travellers' laptops is thing you call the height of it. Despite the need to meet constitutional due process requirements for searching a laptop within the US legal system, the Department of Homeland Security approved the accessing of travellers' computers without judicial authorization.[xxiv] In Nigeria, there were several reports of the defunct Special Anti-Robbery Squad (SARS) of the Nigeria Police Force searching people's mobile phones, laptops and other

digital devices on mere suspicion of being Yahoo boys, a term understood in Nigeria to mean internet fraudsters.[xxv]

It is interesting to note that in most instances states veil themselves with the omnibus shade of national security, national interest and or the fight against terrorism to interfere with and invade privacy, keep terrorist/watch list with limited access to legal safeguards. The same omnibus shade of national security is often invoked to formulate counter-terrorism policy with little or no regard for human rights implications especially the right to privacy. Sometimes in April 2013, Premium Times reported that the Nigerian government planned to purchase equipment that would allow it conduct online surveillance on an unprecedented scale. The same year in May 2013, a report emerged that Citizen Lab, a University of Toronto Research Center discovered that Nigeria and 11 other countries acquired Fin Fisher. It is a surveillance software that has the capability of obtaining password from computers, monitor Skype calls and even remotely turn on computer cameral and sound recording so as to watch the user of the computer remotely.[xxvi] There was also media report that the Nigerian government allocated the sum of 4.8billion naira to the National Intelligence Agency (NIA) to monitor WhatsApp messages, phone calls, text messages, among others.[xxvii] Interestingly, each of cases will be justified by the state under the cover of national security more so that right to privacy is not absolute and it is lawful to derogate from it in the interest of defence, public order or national security. This therefore calls for a balancing of the individual right to privacy vis-à-vis the legitimate interest of the government to maintain national security. In so far as the state authority should have the power to maintain law and order and by extension ensuring an effective national security, there should legal guidance-some sort of permissible limitation test- in place to ensure such power does not arbitrarily interfere with the fundamental right to privacy.

LIMITATIONS TO RIGHT TO PRIVACY AND THE LEGITIMATE INTEREST OF THE GOVERNMENT

No doubt, right to privacy is not without limits. Preponderantly, the law recognizes that right to privacy can be limited or derogated from in certain instance in accordance with the law in the interest of defence, public safety, national security/interest and protection of the right and freedom of others.[xxviii] Meanwhile, the activities of states geared towards the maintenance of

law and order are vicissitudinous and because "national security" is an omnibus term with many shades "national security" becomes a ready defence often invoked by state authorities in defence of an act that may clearly interfere with individual right to privacy. While the right of individuals to privacy is guaranteed by the law, its limit is prescribed and at the same time the government authority also has a legitimate right/interest to maintain law and order in order to guarantee national security. Thus, in the process of state authorities wanting to maintain national security, actions are taken overboard which make those steps end up invading individual privacy.[xxix] This privacy right of the individual and the legitimate interest of the government therefore require some balancing test. This is because without a rigorous set of legal safeguards and a means to measure the necessity, proportionality or reasonableness of the interference, states would have no guidance on minimizing the risks to privacy invasion generated by their policies, actions and activities in the maintenance of law and order and the legitimate pursuit of national security.

BALANCING THE COMPETING INTERESTS BETWEEN INDIVIDUAL RIGHT TO PRIVACY AND THE MAINTENANCE OF NATIONAL SECURITY

Both at the national and international levels, there is a consensus to the effect that right to privacy, like majority of other right, is not absolute[xxx] and this limitation applies regardless of whether the right to privacy is enjoyed offline or applicable online.[xxxi] Nonetheless, it has been preponderantly agreed upon that international human rights laws provide a universal framework upon which any interference with individual privacy right must be assessed.[xxxii] While right to privacy, whether online or offline, is not absolute, any limitation to it must be provided by law. This means that the law providing the limitations should be accessible, precise and clear so much that it enables an individual take a look at the law and ascertain its confines.[xxxiii] Also, if the limitation is in relation to privacy online in which surveillance is authorized, the laws limiting the right, apart from it being required to be accessible, precise and clear to enable an individual ascertain its limits, it must also specify who is authorized to conduct such surveillance and under what circumstances.[xxxiv] In addition, the limitation must be necessary for reaching a legitimate aim and this implies that such limitation that constrains the right to privacy must be proportionate.

It goes without saying that where the act of interference with right to privacy is one that is carried out through surveillance activities, such surveillance must be in proportion to the aim it seeks to achieve and the authority conducting such surveillance should choose the least intrusive option available.[xxxv] It also mean that if it is for the purpose of protecting national security or the right to life and freedom of others, the limitation on right to privacy must be shown to have some chances of achieving the set goal.[xxxvi]

THE PERMISSIBLE LIMITATION TEST

Indeed, the internationally acceptable legal framework for limitations to right to privacy, like every other human right, disallows the states from hiding mischievously under the amorphous provision of "national security" to perpetuate flagrant violation of human rights. The authorities of states that seek to limit right to privacy has an onus to demonstrate that the limitation is really connected to the internationally-acceptable legitimate aims enunciated in various laws. Hence, as much as limitations to right to privacy exist, any of such limitations must be consistent with other human rights and should not render privacy meaningless.[xxxvii]

It is safe to conclude that where states relies on their laws or policies to limit the application of right to privacy relying on any grounds provided by law- "national security" being the usual favourite- the limitations must meet the requirements of legality, necessity, proportionality, adequate safeguard and the principle of access to remedy: victimhood, standing, and notification, failing which such limitation would be unlawful and its interference with the right to privacy would be arbitrary.[xxxviii] Each of these principles is briefly discussed below;

THE PRINCIPLE OF LEGALITY

This principle dictates that the basis of any interference with right to privacy must be legal. In order word, the interference must be done in accordance with the law. The measure to be taken by the state authority must be consistent with its international obligations and such measure must be carried out based on a legal framework. In addition, such legal framework must be publicly accessible,[xxxix] clear, precise, comprehensive, non-discriminatory and not arbitrary; and should be reasonable and of pursuing the legitimate aims.[xl] It follows without saying that

limitations to right to privacy must be established and provided by law.[xli] The law in this regard must be one that results from the deliberation of a legislative body, a parliament, "which precisely defines the causes and conditions that would enable the State to intercept the communications of individuals, collect communications data or "metadata," or to subject them to surveillance or monitoring that invades spheres in which they have reasonable expectations of privacy." In other words, the law should be an act of parliament and not just a mere regulation, policies or directives.[xlii]

PRINCIPLE OF NECESSITY

The principle of necessity dictates that the state authorities must show that the restrictions imposed or the interference with individual right to privacy is merely useful, reasonable or desirable to achieve the government's legitimate interest.[xliii] The state must, in addition, demonstrate the actual nature of the threat because of which it imposes measure which restricts or limits right to privacy as well as the "direct and immediate connection" between the measure imposed and the threat.[xliv]

THE PRINCIPLE OF PROPORTIONALITY

This principle requires that any interference with the right to privacy should be shown to be "a necessary means to achieving a legitimate aim." There must be "a rational connection between the means employed by the state and the aim sought to be achieved." In this regard, it must be demonstrated also that the mean or measure chosen or employed is in the interference with privacy right is s "the least intrusive instrument among those which might achieve the desired result".[xlv] This involves "balancing the extent of the intrusion into … privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest."[xlvi] This balancing will include the need for the state authority to ensure on one hand that the restriction imposed or interference with right to privacy does not end up impairing the essence of the right itself. And on the other hand, ensure that the decision the consequences of which interfere with the right to privacy is taken by the appropriate authority designated by law.[xlvii]

THE PRINCIPLE OF ADEQUATE SAFE GUARD

This principle requires an effective safeguard be emplaced by the state to ensure that information concerning a person's privacy harvested as a result of the interference with the individual's right to privacy does not reach or end up in the hands of "persons who are not authorized by law to receive, process and use such information, and also the state must ensure the information is not "used for purposes incompatible" with the provisions of ICCPR .[xlviii]

In the case of Weber and Saravia v. Germany,[xlix] the European Court of Human Rights held that the Court "has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."

Similarly, in the case of Klass and Others v. Germany,[l] the European Court of Human Rights held to the effect that "the permissible restrictive measures" should be confined to "cases in which there are factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may only be ordered if the establishment of the facts by another method is without prospects of success or considerably more difficult; even then, the surveillance may cover only the specific suspect or his presumed "contact-persons." To this end, the court maintained that "exploratory or general surveillance" is impermissible.

Thus, for a state authority to fulfil this condition, it must be shown that the measure taking is taken in accordance with safeguard, upon reasonable suspicion. It must similarly ensure that there is an effective oversight,[li] that the information is not used for another purpose, and there is transparency.[lii]

PRINCIPLE OF ACCESS TO REMEDY: VICTIMHOOD, STANDING, AND NOTIFICATION

This principle requires the provision of adequate remedies in place for violation of right to privacy. The Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age,[liii] has established that "effective remedies for violations of privacy through digital surveillance can come in a variety of judicial, legislative or administrative forms." This dictates that, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. A person whose right to privacy has been violated should be able to challenge the action of the state authority so that the judicial arm of the government can rule on such action with a view to ascertaining whether the measures adopted by the state which consequently interfere with the individual right to privacy and the interference itself is lawful.

APPLICATION OF THE PERMISSIBLE LIMITATION TEST IN NIGERIAN JURISPRUDENCE

The permissible limitation tests discussed above are in accord with the position of UN HRC, in its General Comments 29,[liv] 31[lv] and 34, considered to be important sources of guidance with regard to permissible limitations to right to privacy. This goes without saying that international best practices require that in balancing the right to privacy with the legitimate interest of the government in the maintenance of law and order, the consequent limitations imposed on or interference with right to privacy should be subjected to the permissible limitations test as in order to such the inference with right to privacy is legal, necessary, proportionate and with adequate safe guard. Now the question is, does this same principle apply in Nigeria when a Nigerian government interferes with right to privacy relying on section 45 of the 1999 Constitution?

One challenge is that Nigeria has not yet domesticate the ICCPR and by virtue of section 12(1) of the 1999 Constitution (as amended).[lvi] This fact alone without more comes with tendency for one to suppose that the permissible limitation test as formulated by human rights court and treaty bodies based on their interpretation of the provisions of ICCPR and other human rights instrument would only be of a persuasive effect in Nigeria. If however, the customary international principle of *pacta sunt servanda* [lvii] is to be considered; and the fact that Nigeria has assented to and ratified a number of human rights instrument including ICCPR,,[lviii] it could

be safely submitted that, Nigeria has an obligation under the international law to apply the provisions of ICCPR. Moreover, it should equally be guided by the interpretation and decisions of treaties and judicial bodies on the provisions of the Covenant. In addition, the preamble to the Fundamental Right (Enforcement Procedure) Rules 2009[lix] empowers the Nigeria courts to respect municipal, regional and international bills of rights cited to it or brought to its attention, or of which the court is aware of for the purpose of advancing but never for the purpose of restricting a party's right and freedom. The bills referred to in the provision is listed to include African Charter on Human and People's Rights, Universal Declaration of Human Rights and other instruments (including protocols) in the African regional and the United Nations human rights system. Consequently, it is our considered view that the permissible limitation tests as formulated by human rights courts and treaties bodies based on their decisions and interpretations of provisions of ICCPR and other human rights instruments to which Nigeria has assented and ratified should apply in Nigeria especially in relation to the rights to privacy. A further extension of this will imply that Nigerian courts can be guided by these permissible limitation tests when deciding an issue bothering on an alleged interference with right to privacy by state authorities.

Therefore, when confronted with the question as to determination of the extent of right to privacy vis-à-vis the reliance of state authorities on national security, Nigerian courts are to bear it in mind and should be ready to scrutinize the states' actions with the finery of the tooth of comb to determine the followings;

1. whether the restrictions imposed by the state is provided by the law,
2. whether the whole essence of a human right is not defeated when subject to such restrictions,
3. whether the restriction is necessary in a democratic society;
4. whether the discretion exercised when implementing the restrictions is unfettered;
5. beyond serving one of the enumerated legitimate aims; whether the restriction is necessary for reaching the legitimate aim;
6. whether the restrictive measures conform to the principle of proportionality in which case the court should determine;
    1. whether it is appropriate to achieve their protective function;

2. whether the measure taken is the least intrusive instrument amongst those which might achieve the desired result; and
3. whether they are proportionate to the interest to be protected because anything short of that constitutes a violation and consequent erosion of right to privacy.

The above will go a long way to establish in the Nigerian jurisprudence that it is not enough for a state to hide under the omnibus shade of national security to violate right to privacy. This will give the needed checks and balances required in the enforcement of law and enjoyment of fundamental right.

CONCLUSION AND RECOMMENDATIONS

The significance of an effective protection of right to privacy in a democratic society like ours cannot be overemphasized. Jurisprudentially, being a fundamental right, right to privacy is a claim right which imposes a negative duty or obligation on others - states and non-state actors - not to intrude or interfere within the sphere of private zones protected by the right. However, when it comes to law enforcement, the state authorities especially often take measures that interfere with or intrude with individual right to privacy. While the individual has a right not to be intruded, the government has a legitimate interest to enforce law and order which more often than interfere with the right to privacy. It is our position that there is a very strong need to always balance the competing interests vis-à-vis right to privacy and law enforcement. Balancing the two will give the state the right to enforce law and order and guarantee national security without eroding individual fundamental right to privacy. It is therefore our recommendations that;

a. States authorities should respect and fulfil their human rights obligations under the international human rights instruments especially as regards right to privacy. If states are willing to respect and fulfil their human rights obligations the incidence of violation of fundamental right especially right to privacy will reduce to the barest minimum.

b. Nigerian judiciary should leverage on the preamble to the Fundamental Rights (Enforcement Procedure) Rules, 2009 to incorporate as part of Nigerian human rights jurisprudence the permissible limitation tests formulated by human rights court and treaties bodies.

c. Whenever the opportunity present itself, the Nigerian courts should always be ready to scrutinize the activities of the state and its reliance on section 45 of the 1999 Constitution in interfering with fundamental right including right to privacy always be guided by the permissible limitation test in balancing the two competing interests. The permissible limitation test is a good legal guidance for the state to respect and protect right to privacy without jeopardizing its duty of law enforcement. Nigeria as a country has a legal framework that can be used by the judiciary to adopted and reflect on the various resolutions/decisions, general comment of the UN Human Rights bodies especially as regards the permissible limitation to test to fundamental rights provisions generally including the right to privacy will undoubtedly enrich our jurisprudence of right to privacy vis-à-vis the omnibus shade of national security.

d. The Human Rights Committee of the United Nations is encouraged and urged to issue a new General Commend in relation to right to privacy guaranteed in article 17 of ICCPR to serve as a new legal guidance for states and judicial bodies. The last one issued by the body was in 1988 before the explosion of the current information revolution. A new general comment by the body especially with respect to right to privacy will go a long way to address new developments in the light of digitations.

ENDNOTES

[i] For instance, Section 45 Constitution of the Federal Republic of Nigeria 1999 as amended.

[ii] Many states also have similar provisions in the body of their laws allowing derogation from right to privacy in the interest of defence, 'sovereignty and integrity of the state', 'friendly relations' (article 19(2) of India Constitution), 'economic wellbeing of the country', (see art. 8 of the ECHR) or 'for the purpose of protecting the rights and freedom of other persons' (section 45, of the 1999 Constitution).

[iii] Adopted in Paris on 10 December 1948. See United Nations General Assembly Resolution 217A http://www.un.org/en/universal-declaration-human-rights/index.html Accessed on 7th September, 2022.
[iv]Adopted by UNGA Resolution 2200A (XXI) of 16 December 1966 www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx. Accessed on 7th September, 2022
[v] Article 8 of the ECHR. This is an international agreement between the 47 States of the CoE in which all the member states of the EU are part of this organization including however third states such as Switzerland, Russia, and Turkey.
[vi] See article 7 of Charter of Fundamental Right of the European Union (2000/C 364/01) < Https://Www.Europarl.Europa.Eu/Charter/Pdf/Text_En.Pdf> Accessed on 14th September, 2022
See article 11 of the American Convention on Human Rights, "Pact of San José, Costa Rica". Signed at San José, Costa Rica, on 22 November 1969< treaties.un.org/doc/publication/unts/volume%201144/volume-1144-i-17955-english.pdf> accessed on 14th September, 2022
[vii] See article 11 of the American Convention on Human Rights, "Pact of San José, Costa Rica". Signed at San José, Costa Rica, on 22 November 1969< treaties.un.org/doc/publication/unts/volume%201144/volume-1144-i-17955-english.pdf> accessed on 14th September, 2022
[viii] See article 10 of the African Charter on the Right and Welfare of the Child. OAU Doc. CAB/LEG/24.9/49 (1990) < achpr.org/public/Document/file/English/achpr_instr_charterchild_eng.pdf> Accessed on 14th September, 2022
[ix] See for instance s37 CFRN, art. 8 ECHR
[x] See art.19(2) India Constitution
[xi] *Ibid.*
[xii] See art. 8 ECHR
[xiii] See s37 CFRN
[xiv] Amnesty International in its report titled: ACTION BRIEF SECURITY WITH HUMAN RIGHTS PROGRAM THE REPORT AND CIA TORTURE" chronicled activities of US authorities in which it accused the US government of violating, on multiple fronts, human rights in the name of national security, often in violation of both U.S. law and international law. https://www.amnestyusa.org/issues/national-security/ accessed on 16th September, 2022
[xv] For instance, President Muhammadu Buhari, the President of the Federal Republic of Nigeria was reported to have said sometimes in 2018 that "The rule of law must be subjected to the supremacy of the nation's security and national interest" https://www.sunnewsonline.com/national-security-cant-be-sacrificed-for-rule-of-law-buhari accessed on 16th September, 2022
[xvi] Deutsche Welle World, 'Germany stops journalist spying in wake of scandal' Deutsche Welle (Germany, 15th May 2006) https://www.dw.com/en/germany-stops-journalist-spying-in-wake-of-scandal/a-2020104> 9th September, 2022
[xvii] Australian Transaction Reports and Analysis Centre, AUSTRAC Annual Report 2018-2009 https://www.austrac.gov.au/about-us/corporate-information-and-governance/reports-and-accountability/annual-reports> Accessed on 8th September 2022.
[xviii] See Financial Transaction and Reports Analysis Centre of Canada, FINTRAC Annual Report 2008, 11 September 2008https://www.publicsafety.gc.ca/lbrr/archives/cn000029669116-2008-eng.pdf Accessed on 9th September, 2022
[xix] Fundación Karisma Dejusticia, 'State of Privacy Colombia' < https://privacyinternational.org/state-privacy/58/state-privacy-colombia> Accessed on 9th September, 2022
[xx] V. Prevelakis and D. Spinellis, 'The Athens Affair' [2007] (24) Spectrum IEEE; 26-34. https://www.researchgate.net/publication/3001282_The_Athens_Affair Accessed on 9th September, 2022
[xxi] Association for Progressive Communication, 'E-Bangladeshi: Crackdown on Internet Users in Bangladesh' (Dhaka, Bangladesh, 05 October 2007) http://www.e-bangladesh.org/2007/10/03/crackdown-on-internet-users-in-bangladesh/ accessed on 9th September, 2022
[xxii] See British All Party Parliamentary Group on Privacy, Briefing Paper: Inquiry into communications data surveillance proposals and the Interception Modernisation Programme, June 2009https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/imp/imp_briefing.pdf Accessed on 10 September, 2022
[xxiii] S. B. Bossa and T. Mulindwa. 'The Anti-Terrorism Act, 2002 (Uganda): Human Rights Concerns and Implications' (A Paper Presented on September 15, 2004 to the International Commission of Jurists)

https://www.icj.org/wp-content/uploads/2012/04/icj_anti-terrorism_act_position_paper_2002.pdf> Accessed on 4th January 2019

[xxiv] See the Department of Homeland Security, Privacy Impact Assessment for the Border Searches of Electronic Devices, 25 August, 2009 https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf accessed on 5th January 2019

[xxv] J. Okafor, 'Nigerians Campaign to #endSARS Over Abuse' All Africa Global Media (Nigeria, 16th December 2017<allafrica.com/stories/201712060197.html> Accessed on 4th December 2019.

[xxvi] E. Nwachukwu and D. Burbidge 'Nigerian Government to Ramp up Internet Surveillance? <'https://www.google.com/amp/s/advox.globalvoices.org/2013/07/12/nigerian-government-to-ramp-up-Internet-surveillance/amp/ > accessed on 10th September, 2022

[xxvii] https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html accesed on 10th September, 2022

[xxviii] See section 45 of the 1999 Constitution of Nigeria (as amended), article 8(1) of the ECHR and article 52(1), (2) and (3) of the Charter of the fundamental rights of the EU, articles 29 and 30 of UDHR and articles 41 and 51 of the ICCPR etc.

[xxix] For instance, between 8th – 9th September, 2022, the Department of State Security Services (DSS) of the Nigerian government raised the residence of Tukur Mamu arrested in connection with the allegation of terrorism. Before his withdrawal from the negotiation and arrest by the DSS, Tukur Mamu was reportedly one of the negotiators between the victims' family and the terrorists that attacked the 28th March, Abuja-Kaduna bound AK-9 train passengers where scores of passengers were kidnapped in Nigeria. During the raid, the residences of the in-laws to Tukur Mamu were also raised. The report indicated that the DSS could not find anything incriminating in the residence of Ibrahim Husaini Mamu, Tukur Mamu's in-law once residence was also raided. Can the raid on Ibrahim Husaini Mamu's residence be lawful under the eye of the law or a clear invasion of privacy? Godwin Isenyo, DSS raids Mamu's in-law, other family members' residences (Punch Newspaper Online, 29th September, 2022) < https://punchng.com/dss-raids-mamus-in-law-other-family-members-residences/> Accessed on 17th September, 2022

[xxx] Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994) <hrlibrary.umn.edu/gencomm/hrcom16.htm#:~:text=HRI%2FGEN%2F1%2FRev, on%20his%20honour%20and%20reputation.> accessed on 17th September, 2022.

[xxxi] U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

[xxxii]UN General Assembly Resolution 68/167, Resolution adopted by the General Assembly on 18th December 2013https://undocs.org/pdf?symbol=en/a/res/68/167 Accessed on 2nd September, 2022. See also U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014) https://privacyinternational.org/sites/default/files/201712/Guide%20to%20International%20Law%20and%20Surveillance%20August%202017.pdf accessed on 17th September, 2022

[xxxiii] *Ibid*.

[xxxiv] *Ibid*.

[xxxv] *Ibid*.

[xxxvi] *Ibid*.

[xxxvii] See the case of Taylor-Sabori v. The United Kingdom, App. No. 47114/99, European Court of Human Rights, Judgment (22 October 2002) where the court declared as constituting an undue interference the surveillance carried out by the police. The court stressed that the phrase "in accordance with the law" in the ECHR requires compliance with not only the domestic law but the quality of such should as well be compatible with the rule of law. This implies that the domestic law to be relied upon must provide protection against arbitrary interference with an individual's right under Article 8 of the Convention and also it must be clear in its terms of giving the individuals an adequate indication as to the conditions and circumstances in which the public authority may resort to such measure limiting the individual right to privacy.

[xxxviii] See the Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014) "…Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article

25 of the International Covenant on Civil and Political Rights. It is our considered that view that the Lawful Interception of Communications Regulations, 2019. B105-118 Federal Republic of Nigeria Official Gazette No. 12 Lagos - 23rd January, 2019 Vol. 106 issued by the Nigerian Communications Commission may not meet the international standard in this regard because it is neither a law envisaged under section 45 and 318 of the 1999 Constitution but rather a regulation which did not pass through the rigour of parliamentary debated before its issuance.

[xxxix] See the case of Malone v. The United Kingdom, App. No. 8691/79, European Court of Human Rights, Judgment (2 August 1984)

[xl] U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

[xli]See the concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015)

[xlii]According to the Office of the Special Rapporteur for Freedom of Expression of the According to the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013).

[xliii]See the case of Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

[xliv]See John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, Brief of Amici Curiae, United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal, D.C. Ct. App., Case No. 16-7081, pp. 14-15, 17-18 (1 November 2016)

[xlv]See the Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014) "51.

[xlvi]*Ibid*

[xlvii]See the case of Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

[xlviii]U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 April 1988) "10.

[xlix]App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

[l]App. No. 5029/71, European Court of Human Rights, Judgment (6 September 1978)

[li] U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014). See also Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

[lii] Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7 (28 April 2016)

[liii]U.N. Doc. A/HRC/27/37 (30 June 2014) "40

[liv] UNHRC, CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency, 31 August 2001, CCPR/C/21/Rev.1/Add.11https://www.refworld.org/docid/453883fd1f.html Accessed 2nd September, 2022

[lv]UN HRC, General Comment No. 31 [80], The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 26 May 2004, CCPR/C/21/Rev.1/Add.13https://www.refworld.org/docid/478b26ae2.html 2nd September, 2022

[lvi] See section 12(1) 1999 Constitution which provides thus: (1) No treaty between the Federation and any other country shall have the force of law except to the extent to which any such treaty has been enacted into law by the National Assembly.

[lvii]The principle is codified under articles 26 and 27 of Vienna Convention on the law of Treaties. Article 26 titled: "Pacta sunt servanda" provides thus: "Every treaty in force is binding upon the parties to it and must be performed by them in good faith. Article 27 also provides thus: "Internal law and observance of treaties A party may not invoke the provisions of its internal law as justification for its failure to perform a treaty. This rule is without prejudice to article 46."

[lviii] Nigeria ratified ICCPR on 29th July, 1993https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=127&Lang=EN accessed on 19th September, 2022

[lix] The rules were made pursuant to section 46(3) of the Nigerian 1999 Constitution (as amended).