EXAMINATION OF THE CONSTITUTIONAL AND HUMAN RIGHTS ISSUES IN CYBERSPACE*

Abstract
The involution and dependence on technology in the present era as well as the increasing access to the internet by all and sundry have given opportunities for the recognition and protection of new sets of fundamental human rights either at the international and National level. The rights already in existence protect rights of individuals in the cyber space as well. This paper focuses on the various forms of rights available in the cyber space and the extent of their protection by any existing legal framework, and whether individuals have any right of enforcement of these rights. The researcher adopts the doctrinal method of research mythology by identifying the various laws protecting fundamental rights in the cyber space both at the international level and local authority with particular focus on Nigeria. The researcher however finds that there are uncertainties and limitations derived from the fact that a plurality of state and non-state actors may limit and interfere with human rights in cyberspace. The researcher recommends that there is need for the Nigerian government to focus on reviewing and strengthening existing laws and enacting appropriate cyber space laws that guarantee the rights of individuals online and punishment for the wrong committed in the cyber space.

Keywords: Constitutional, Cyberspace, Cybercrime, Freedom of Speech and Expression, Human Rights, Investigation, Jurisdiction and Privacy

1. Introduction

Human rights are rights inherent to all human beings, whatever their nationality, place of residence, sex, national or ethnic origin, color, religion, language or any other status. We are all entitled to our human rights without discrimination. These rights are interrelated, interdependent and indivisible. Human rights in cyberspace are relatively new and uncharted area of law. The United Nations Human Rights Council (UNHRC) has stated that the freedom of expression and information under Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR) include the freedom to receive and communicate information, ideas and opinions through the internet. As policy areas, cyberspace and human rights have become so intertwined that understanding one requires sustained attention to the other. This observation holds even though human rights are not dependent on any technology, and the technologies producing cyberspace have no 'hard wired' ideology. This paper analysis the relationship between cyberspace and human rights particularly the following rights; (a) freedom of speech and expression, (b) Right to Access the Internet, (c) Right to privacy and (d) Right to data protection. The relationship has evolved from early visions of cyberspace as an unprecedented realm for human rights to today's struggles to protect rights in a cyberspace by divergent interests colliding in a multipolar world increasingly dependent on cyber technologies.

The human rights consequences of the internet's emergence are apparent in two contexts. First, cyber space challenges general principles of international law important for human rights, including sovereignty, non-intervention and jurisdiction. Second, cyberspace emerges in the human rights regime, institutions and processes associated with protecting human rights. The human rights footprint of cyberspace is so large that experts debate whether internet access is, or should be, a new human right.[1] In the case of human rights issues in the cyber world, there are some provisions about the rights and principles of internet freedom, as shown on the official website *'Internet Rights & Principles Coalition'*[2], explaining the 10 principles and human rights on the internet;

a. Universality and Equality. All humans are born free and equal in dignity and rights which must be respected, protected and fulfilled in online environment;
b. Rights and social justice. The internet is a space for the promotion, protection and fulfillment of human rights and the advancement of social justice. Everyone has the duty to respect the human rights of all others in the online environment;
c. Accessibility. Everyone has an equal right to access and use a secure and open internet.
d. Speech and Association. Everyone has the right to seek, receive and impart information freely on the internet without censorship or other interference. Everyone also has the right to associated freely through and on the internet, for social, political and cultural or other purposes;
e. Privacy and Data Protection. Everyone has the right to privacy online. This includes freedom from surveillance, the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure;

***By Balkisu ALIYU,** Lecturer, Gombe State University, Faculty of Law. E-Mail: barrbilkisua@gmail.com. Phone No: 08156443024

[1] David P Fidler, Research Handbook on International law and cyberspace (2015) <http://scholar.google.com/scholar?hl=en&as_sdt+0%2C5&q=human rights issues in cyberspace> accessed 18 March 2022

[2] Diana Lukitasari, 'Freedom of speech in cyberspace in Human rights protection perspective' {2013} vol 2 Iss 3 *IJBEL* 79

f. Life, Liberty and Security. The rights to life, liberty and security must be respected, protected and fulfilled online. These rights must not be infringed upon, or used to infringes other rights, in the online environment;
g. Diversity. Cultural and linguistic diversity on the Internet must be promoted and technical and policy innovation should be encouraged to facilitate plurality of speech;
h. Network Equality. Everyone shall have universal and open access to the internet's content, free from discriminatory prioritization, filtering or traffic control on commercial, political or other grounds;
i. Standards and Regulation. The internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion and equal opportunity for all;
j. Governance. Human rights and social justice must form the legal and normative foundations upon which the internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation and accountability. [3]

2. Freedom of Speech and Expression in Cyberspace

The idea of freedom of speech had originated a long time ago. It was first introduced by the Greeks. They used the term 'Parrhesia' which means *'free speech or to speak frankly'*. This term first appeared in the 5th century B.C. Countries such as England and France have taken a lot of time to adopt this freedom as a right. The English Bill of Rights, 1689 adopted freedom of speech as a constitutional rights and it is still in effect. Similarly, as the time of the French Revolution in 1789, the French had adopted the Declaration of the Rights of Man and of Citizens. [4] The UN General Assembly adopted the Universal Declaration on Human Rights on 1oth December 1948 and under Article 19, freedom of speech and expression was recognized as one of the human rights. The cyber world has a major role in the stand-up for human rights, especially the rights of opinion implemented by speech through cyberspace. The cyberspace is a means to communicate without limits, thus it is granted to create a sense of justice and the protection in the freedom of opinion only if the user rights or user service is regulated in order to implement their right without any fear. This does not however make an excuse to restraint of freedom of speech in society.

Freedom of speech is a part of human rights, which freedom is manifested from the submission orally or written in any media without any obstruction from any party. Speech is a form of opinion. A freedom of speech is recognized as a basic human rights and gets protection assurance in the Universal Declaration of Human Rights (UDHR) 1948. In Article 19 of the UDHR which states thus:

> Everyone has the right to freedom of thought and speech (the right to freedom of opinion and speech), the right shall include freedom to hold an opinion without interference and the freedom to seek, receive, and impart information and ideas, through any media regardless of state boundaries.[5]

From the above provisions, it can be seen that in order for the freedom of opinion to be implemented well, then it must be given assurance and immunity, so individuals are not afraid of the retaliation of any party[6]. However there are some restrictions on the freedom of speech. In any system of international and national human rights, it is recognized that freedom of speech can be restricted only to a very limited criteria, and should be made with great care and must be in accordance with the International Covenant on Civil and Political Rights (ICCPR)[7]. Article 19(3) of the ICCPR provides thus:

> The exercise of the right provided in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subjected to certain restrictions, but these shall only be such as are provided by law and are necessary;
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order, or of public health and *morals.'*

In other words, the restrictions are authorized when they are in pursuit of a legitimate aim, in accordance with existing law, and necessary and proportionate to the threat that justified their implementation. The restrictions are important because when the freedom of speech is not regulated, it can interfere with other rights stipulated by the United Nations such as right to be free from cruel, inhuman or degrading treatment, right to privacy, freedom from discrimination and the right of children to special protection. As a member of the United Nations and a state

[3] Internet Rights & Principles Coalition 2013. 10 Internet Rights & Principles <https://internetrightsandprinciples.org/campaign> accessed 18 March 2022
[4] Subodh Asthana, 'Freedom of Speech and Expression' https://blog.ipleaders.in/freedomspeechexpression/amp/ accessed 22 March 2022
[5] See also Article 10 of the European Convention on Human Rights of 1950; Article 19 of the International Covenant on Civil and Political Rights of 1966; Article 9(2) of the African Charter on Human and Peoples' Rights of 1981.
[6] (n.2) 80
[7] (n.2) 80

party to the UDHR, Nigeria cannot let go of taking moral and legal responsibility to uphold and implement the UDHR stipulated by the United Nation.

In the light of the above, in 1999 Constitution of the Federal Republic of Nigeria (as amended), protection of right to Freedom of speech is specifically guaranteed and regulated in section 39 under Chapter IV of the. It reads thus:

> (1) Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference.
> (2) Without prejudice to the generality of subsection (1) of this section, every person shall be entitled to own, establish, and operate any medium for the dissemination of information, ideas and opinions:
> Provided that no person, other than the Government of the Federation or of a State or any other person or body authorized by the president on the fulfillment of conditions laid down by an Act of the National Assembly, shall own, establishment or operate a television or wireless broadcasting station for any purpose or whatsoever.
> (3) Nothing in this section shall invalidate any law that is reasonably justifiable in a democratic society.
> (a) for the purpose of preventing the disclosure of information received in confidence, maintaining the authority and independence of courts or regulating telephone, wireless broadcasting, television or the exhibition of cinematograph; or
> (b) imposing restrictions upon persons holding office under the Government of the Federations or of a State, members of the armed forces of the Federation or member of the Nigeria Police Force or other Government security services or agencies established by law.[8]

In essence, freedom of speech is available to citizens in Nigeria. This right is regarded as one of the most basic elements of a healthy democracy because it allows citizens to participate in the social and political process of a country actively. The Human Rights Council further states that the rights that people have offline must also be protected online particularly freedom of expression and this right must be balanced with other rights.[9]

Taking a cursory look at the tussle in Nigeria between banning Twitter, The Government and its citizens, it is clear that the issue of right to freedom of speech guaranteed under the 1999 Constitution as well the various International Conventions to which Nigeria is a signatory, a basic right inherent in citizens can only be enjoyed if it favors the Government (my opinion though). It is correct that the 1999 Constitution has certain restrictions when it comes to freedom of Speech and press, however, those restrictions are limited to Television and Radio Broadcasting and not an online platform or site where citizens explore their basic human rights to speak freely without consequence. The Nigeria Broadcasting Commission Act regulates the broadcasting sector in Nigeria and established a Commission responsible for implementing the provisions of the Act by ensuring compliance. It did not in any way make provision for regulating online media or platform.[10] The Minister of Information and Culture, Mr. Lai Mohammed, during a session organized on 15th June, 2021 by the House Committees on Information, Ethics and Values aired on Channels television at 10:00pm News broadcast to inquire as to the decision of the Federal Government to ban Twitter in Nigeria coincidentally after Twitter took down one of the post of the President, asked the members to include online and internet broadcasting under the control of the Nigeria Broadcasting Commission (NBC). The implication is that once online and internet broadcasting is regulated by NBC, it would amount to taking away the civic space, freedom of expression and media freedom in Nigeria which is in contravention to section 39 of the 1999 Constitution (as Amended). Nigerian citizens are free to express their opinion on any matter in the country (which operates democratic system of government) and can use whatever medium they so desire to do so without any form of fear or oppression (see Sections 39 (2) of the 1999 Constitution).

3. Right to Access Cyberspace (Access to Internet)

The right to internet access, also known as the right to broadband or freedom to connect, is the view that all people must be able to access the internet in order to exercise and enjoy their rights to freedom of expression and opinion and other fundamental human rights, that states have a responsibility to ensure that internet access is broadly available and that state may not unreasonably restrict an individual's access to internet.

In December 2003, the World Summit on the Information Society (WSIS) was convened under the auspice of the United Nations. After a lengthy negotiation between governments, businesses, and civil society representatives, the WSIS Declaration was adopted, reaffirming the importance of the Information Society in maintaining and strengthening human rights[11]. The Declaration of Principles reads thus[12]:

[8] CFRN 1999 (as amended)
[9] Wikipedia, 'Human Rights in Cyberspace' Http://en.m.wikipedia.org/humanrightsincyberspace accessed 22 March 2023
[10] The recent case of NBC suspending Channels TV with N5million fine <https://guardian.ng/news/nigerian-government-suspends-channels-tvs-politics-today/ accessed 11th April 2022
[11] Wikipedia, 'Rights to internet Access' https://en.m.wikipedia.org/wiki/righttointernetaccess/ accesses 22 March 2022
[12] ibid

> 1. We, the representatives of the peoples of the world, assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to building a people-centered, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.
> 3. We reaffirm the universality, individuality, interdependence, an interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration. We also reaffirm that democracy, sustainable development, and respect for human rights and fundamental freedoms as well as good governance at all levels are interdependent and mutually reinforcing. We further resolve to strengthen the rule of law in international in national affairs.

The WSIS Declaration of Principles also makes specific reference to the importance of the right to freedom of expression which is intertwined with the right to access the internet by stating thus[13]:

> 4. We reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Similarly, in May 2011, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression submitted a report to the UN Human Rights Council titled 'Exploring key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds of media.' The report made 88 recommendations on the promotion and protection of the right to freedom of expression online, including secure access to the internet for all citizens. Other recommendations call on states to respect online anonymity, adopt privacy and data protection laws and decriminalize defamation[14]. The salient points of the Report are:

a. There are two facets to the internet. The first concerns access to online content, with only a few permitted restrictions. The second concerns the availability of the necessary infrastructure and ICTs to be able to access the internet;
b. The internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as stated in Article 19 of the UNDHR and ICCPR;
c. The Special Rapporteur confirms that Article 19 was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression;
d. The right to freedom of opinion and expression is not only a fundamental rights of its own accord but is also an enabler of other rights including economic, social and cultural rights, such as the right to education and the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications, as well as civil and political rights, such as the rights to freedom of association and assembly;
e. By acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the internet also facilitates the realization of other human rights;
f. All states, therefore have a positive obligation to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise right, which therefore includes the internet, by adopting effective and concrete policies and strategies…to make the internet widely available, accessible and affordable to all;
g. The Report also states that the internet, as a medium by which the right to freedom of expression can be exercised, can only serve its purpose f states assume their commitment to develop effective policies to attain universal access to the internet. And given that the internet has become an indispensable tool for realizing a range of human rights…ensuring universal access to the internet should be a priority for all States.[15]

Some countries around the world have adopted laws that require the State to work to ensure that internet access is broadly available. Some of the countries include; Costa Rica, Estonia, Finland, France, Greece, India, Spain, European Union etc. In the summer of 2016, the UN declared that it considers the internet to be a human right.

[13] (n.9)
[14] (n.9)
[15] (n.9)

Specifically, an addition was made to Article 19 of the UDHR which states thus[16]: 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media ad regardless of frontiers'. There were several countries opposed to the amendments including Russia, China, Saudi Arabia, Indonesia, India and South Africa. These countries contested the language that condemned any measures to disrupt internet access or hinder the sharing of information online. However, this language was crucial to the document's implementation and was approved in spite opposition. Article 19 is still considered a 'soft law' in that it only recommends actions for nation-states and lacks any enforcement mechanisms as a hard law would. The Declaration and the Report are non-binding documents of the UN. They only serves as a wakeup call for every country, whether developed or developing. Since the right to internet access in interwoven with the right to freedom of speech and opinion, Section 39 of the 1999 Constitution equally applies and thus guarantees the right to internet access. Section 39(2) provides thus: (2) Without prejudice to the generality of subsection (1) of this section, every person shall be entitled to own, establish, and operate any medium for the dissemination of information, ideas and opinions:

From the above provision, it is evident that Nigerian citizens are free to express their opinions and ideas through any means they so desire, hence online platform falls within the ambit of *'any medium'.* On that note, Right to access the internet is a right guaranteed under the 1999 Constitution and must be enjoyed by the citizens.

4. Right to Privacy

The recognition of privacy is deeply rooted in history and religion. There is recognition of privacy in both the holy Quran (Q24:27 and 28) and the Bible. Over 50 years ago, George Orwell, the English writer imagined a totalitarian state where advanced technologies would be used to monitor the people in all their endeavors[17]. The new technologies have enhanced the possibilities of invasion into the privacy of individuals and provided new tools in the hands of eavesdroppers. Individual privacy is at a greater stake than ever before. Computers and the internet can be used to amass huge amount of data regarding people, profile in various ways, commodify it and deal with it in a manner which could violate individual's privacy.[18] The legal right to privacy is constitutionally protected in most democratic societies. This constitutional right is expressed in a variety of legislative forms. Examples include ICCPR, UDHR, ECHR, USA privacy Act (1974), the Constitution of Federal Republic of Nigeria 1999 (As Amended) and the Data Protection Act in England. The Organization for Economic and Coordination and Development (OECD) also accepted in 1980 the Guidelines for the protection of Privacy and Trans-Border Flow of Personal Data[19].

Privacy is an important right because it is a necessary condition for other rights such as freedom and personal autonomy. Respecting a person's privacy is to acknowledge such a person's right to freedom and to recognize that individual as an autonomous human being. Privacy is the interest that individuals have in sustaining a personal space, free from interference by other people and organisations. The right to privacy refers to specific right of an individual to control the collection, use and disclosure of personal information. Personal information may be in the form of habits and activities, personal interest, family records, medical records, educational records and communication (mails, chatting and telephone) records and financial records etc. The evolution of technologies has produced a different set of issues relating to privacy rights and data protection. These technologies make personal data easily accessible and communicable.[20] The level and varying nature of transactions carried out online are such that the right to privacy must exist at least to a limited extent, the nature of the transaction raises the issue of political, economic and social security of a nation, as such there is great concern about the abuse of information gathered and privacy concerns. The privacy of individuals is a concern of the law. This basic right to protect an individual's privacy has been enshrined in the Universal Declaration of Human Rights[21] (UDHR). Article 12 provides thus; 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference and attacks.' This human right has also been articulated in the International Covenant on Civil and Political Rights[22] (ICCPR). Article 17(1) stipulates: 'No one shall be subjected to arbitrary or unlawful Interference with his privacy, family, home or correspondence nor to unlawful attacks upon his honour and reputation. Article 17 (2) states: 'Everyone has the right to the protection of the law against such interference

[16]Catherine Howell and Darrell M. West, 'The Internet as a Human Right' (2016) Techtank https://brookings.edu/blog/techtank//2016/11/07/theinternetasahumanright/ accessed 22 March 2021

[17] Raman Mittal and Neelotpal Daka, 'Cyber Privacy: Legal Dimensions of Cyberspace' 197

[18] Ibid

[19] Collier, G. (1994). 'Information Privacy': Just how private are the details of individuals in a company's database? *Information management and computer security*, vol. 3 (1) p.41-45.

[20] Supra note 2,

[21] Universal Declaration of Human Rights 1948 (UDHR).

[22] International Covenant on Civil and Political Rights 1976 (ICCPR). This covenant was adopted by the United Nations General Assembly on 16th Dec. 1966 and entered into force on 23rd March 1976. By the end of 2001 the covenant had been ratified by 147 states.

and attacks'. The ICCPR requires the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks, as well as to the protection of this right.

Similarly, the European Convention on Human Right[23] under Article 8 (1) stipulates thus: 'Eeveryone has the right to respect for his private and personal Life, his home and his correspondence'. According to Article 8(2) 'there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in Democratic society in the interests of national security, public safety or the economic well-being of the country….' According to the decision of European Court of Human Rights, the interception of private communications by a government agency in order to draw up a personal profile of a person subject to the interception has been held to constitute an interference with that person's right under Article 8 of ECHR.[24] Article 7 of the 2000 Charter of Fundamental Rights of the European Union provides that 'everyone has the right to respect for his or her private and family life, home and correspondence'. The US Constitution does not explicitly provide for right to privacy, however Supreme Court decisions over the years have established that the right to privacy is a fundamental human right and as such is protected under the 9th amendment[25]. The US do not have comprehensive law on privacy protection, the federal laws covers some specific categories of personal information which includes financial, credit, educational, motor vehicle registration records[26] and children online activities[27]. In the UK several steps have been taken with respect to the internet privacy. The Data Protection act, 1998 was enacted for implementing the European Union Data Protection Directive[28], which is the key to the issues of internet privacy in Britain. The Data Protection Act is concerned with personal data which an individual can be identified form that data or information in the possession of the data user[29].

The Nigerian Constitution[30] however, provided for the right to privacy under Section 37 and it reads thus; 'The privacy of citizens, their homes, correspondence, right to telephone conversations and telegraphic communications is hereby private and guaranteed and protected'. Looking at the recent controversy on the allegation that the Nigerian Communications Commission (NCC) tracked and leaked the telephone conversation between Bishop David Oyedepo, the general overseer of the Living Faith Church and Peter Obi, the candidate of the Labour Party in the 2023 presidential election, Nigerians are questioning how safe their private telephone conversations are.[31] Notwithstanding, the NCC had denied tracking and leaking the phone calls of Nigerians[32], it has however recently said that the Office of the National Security Adviser (ONSA) has a direct link to the NCC's SIM registration data base in order to monitor and apprehend criminals in the country.[33] These kinds of controversies surrounding the right to privacy in cyberspace; the collection and use of personal data by technology companies and governments; government surveillance and mass data collection in the name of national security; and the use of data by social media platforms and other online services for targeted advertising and manipulation of user behaviors around the world[34], has made many internet users concerned about how their personal information, such as their browsing history, online activities, and social media posts, are collected, stored, and used by various entities without their explicit consent. This has led to debates about the need for stricter regulations and laws to protect individuals' privacy online. The right to privacy in cyberspace is a complex and controversial topic that involves multiple stakeholders, including individuals, technology companies, governments, and policymakers. Finding a balance between privacy and other interests, such as security and business, is a challenging task, and debates on this issue are likely to continue as technology continues to evolve.

5. Right to Data Protection

The digitalization of information has caused unprecedented possibilities for the identification of individuals through their data. Personal data are processed by an ever-growing number of private and public instances

[23] European Convention of Human Right 1950 (ECHR) as amended by protocol No II (ETS NO. 155), as from the date of its entry into force on 1 Nov. 1998. As from that date, Protocol No. 9 (ETS No. 140) which entered into force on 1 October.
[24] *Amann v. Switzerland* (GC), no. 27798/95, ECHR 2000-II, pp. 69-70.
[25] *Griswold v. Connecticut* (1965)382 U.S 479. And Katz v. United States (1967) 389 U.S 317.
[26] R.K. Chaubey, ' An introduction to Cybercrime and Cyber security' (Kamal Law House, Kolkata), chapter 5, p. 908
[27] Children Online Privacy Protection Act of 1998.
[28] EU Directive 95/46/EC
[29] Supra note 11,
[30] Constitution of the Federal Republic of Nigeria 1999(As Amended).
[31] Read more on <https://www.legit.ng/politics/1528838-leaked-audio-ncc-tracks-peter-obis-phone-conversation-oyedepo-fresh-fact-emerges/ and < 'How Safe Are Your Phone Calls?', Peter Okoye Asks Nigerians Amid Obi 'Leaked Call' Saga - TheNigeriaLawyer accessed 12th April 2022
[32] <https://www.lindaikejisblog.com/2023/4/ncc-denies-tracking-and-leaking-phone-calls-of-nigerians-2.html accessed 12th April 2022
[33] Prof Umar Garba Danbatta, NCC's executive vice chairman, who was represented by Mr. Tony Ojobo, director, Public Affairs, NCC, stated this when the commission hosted a delegation of students from the US war College in Abuja. < https://technologymirror.com.ng/ncc-confirms-fg-monitoring-of-phone-calls-in-nigeria/ accessed 12th April 2022
[34]<https://www.researchgate.net/publication/333448938_Challenges_in_Cybersecurity_and_Privacy_-_the_European_Research_Landscape accessed 12th April 2022

globally. Personal information is put into cyberspace by users themselves as well as third parties. Individuals leave identity traces through their use of information and communication technologies (ICT). Profiling of Internet users has become a wide phenomenon and Companies sometimes control employees and business contacts through ICT. In addition to national data protection laws, a range of data protection instruments have been adopted at an international level. The most influential of these have been worked out under the auspices of European Union (EU), Council of Europe (CoE) and Organisation for Economic Co-operation and Development (OECD). These instruments are:

i. the European Union's Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data[35], adopted by the European Parliament and the Council on 24/10/1995;
ii. the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[36] adopted by the CoE Committee of Ministers on28.1.1981; and
iii. the OECD's Guidelines Governing the Protection of Privacy and Trans border Flows of Personal Data[37] adopted by the OECD Council on 23.9.1980.

The United Nations (UN) has also issued Guidelines Concerning Computerized Personal Data Files[38]adopted by the UN General Assembly on 4.12.1990. These guidelines, however, have received relatively little attention.
The fundamental human right to respect for private and family life, home and correspondence as guaranteed by Article 8 of the European Convention on Human Rights includes the right to the protection of personal data as well as the obligation to establish appropriate safeguards under domestic law in this regard. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention No 108') requires that personal data be processed fairly and securely for specified purposes on a legitimate basis only, and establishes that everyone has the right to know, access and rectify their personal data processed by third parties or to erase personal data which have been processed without right[39].

What is data protection?
It is the safeguarding of the privacy rights of individuals in relation to the processing of their personal data. You supply information about yourself to government bodies, banks, insurance companies, medical professionals and many others in order to avail of services or satisfy obligations. Organisations or individuals also obtain information about you from other sources. For the purpose of data protection such organisations or individuals who control the contents and use of personal data are known as data controllers. The Data Protection Acts 1988 and 2003 give you rights relating to this personal information and impose obligations on data controllers. These rights apply where the information is held:
- on computer, or
- in a manual form, as part of a filing system that facilitates ready access to a specific individual's information[40].

OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data
The OECD Guidelines on the Protection of Privacy and Trans-border flows of Personal Data, were developed by OECD Member countries in 1980 and were revised in 2013 to provide a risk-management approach as well as a discussion on the importance of developing international interoperability in ensuring privacy. OECD's members are given a framework of guidelines as well as suggestions for implementation. The Guidelines were formed to help harmonize national privacy legislation and while upholding human rights, at the same time prevent interruptions in international flows of data and the guidelines attempt to balance the protection of privacy and individual liberties and advancement of free flows of personal data through eight privacy principles which if observed, are supposed to guarantee a free flow of personal information from other OECD countries. The principles are as follows:
Collection Limitation Principle: Personal data should only be collected lawfully and fairly and where appropriate with knowledge and consent of the individual concerned[41].
Purpose Specification Principle: The purposes for which personal data are collected should be specified at the time of or before data collection. Subsequent use of such data is limited to the purpose of collection or a compatible purpose and that these should be specified whenever there is a change of purpose[42].

[35] Directive 95/46/EC (OJ No L 281, 23.11.1995, 31) – hereinafter termed 'EU Data Protection Directive' or'DPD
[36] ETS No 108 – hereinafter termed 'CoE Data Protection Convention'. The Convention entered into force on 1.10.1985.
[37] Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data (Paris: OECD, 1980
[38] Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20.2.1990).
[39] Council of Europe 'protection of privacy and personal data on the internet and social media' Report of Committee on Culture, Science and Education. Rapporteur: Mrs Andreja RIHTER, Slovenia, Socialist Group. Doc 2011.
[40] Supra note 5.
[41] OECD Guidelines Article 7
[42] Ibid. Article 9

Use Limitation Principle: Restricts the disclosure of personal information for reasons other than the specified purpose except with the individual's consent or by legal authority[43].

Other principles in the Guidelines include:
Personal data should be protected by reasonable security safeguards;
Openness about practice, policies, and developments regarding the data; governments should be open about policy developments and practices with respect to personal data;
Specified set of rights for the individuals from whom data is collected individuals should be able to request data about themselves and receive reasons for denial of such requests;
Accountability of the data controller data controllers should be accountable for complying with the principles[44].

European Union
The Council of Europe Convention was the first binding international instrument to protect individuals against abuses resulting from the collection and processing of personal data and to regulate the trans-border flow of personal data. Many of the principles reflect those of the OECD Guidelines. Countries from outside Europe can sign up to the Convention[45]. The European parliament and the Council of the European Union passed the Data Protection Directive with an aim to establish a regulatory frame work to protect privacy through meeting three stated objectives. The objectives include protection of the rights and freedoms of individuals regarding the processing of personal data, harmonization of datas protection standards throughout Europe and to limit movement of data to those countries outside of Europe that do not have adequate levels of protection. The directive aimed at facilitating the development of e-commerce by fostering consumer confidence and minimizing differences between member States data protection rules. The directives require E.U member States to adopt national legislation ensuring privacy protection if they wish to participate in the free flow of information within the European Union. Article 2(a) of the EU Directive 95/46 and Article 8 of the African Union Convention on Cyber Security and Personal Data Protection provide thus: 'Personal data' shall mean any information relating to an identified Natural person (data subject): an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.' Article 25 establishes the general rule, that data should only be transferred to a non-EU country if they will be adequately protected there[46].

The Human Rights Committee's General Comment No.16 on the right to privacy under the ICCPR clarifies in paragraph 10 that: 'The gathering and holding of personal information on computers, data banks And other devices, whether by public authorities or private individuals or bodies must be regulated by law….in order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes'.
Article 8 of the 2000 Charter of Fundamental Rights of the European Union protects personal data. It reads thus:

> (1) Everyone has the right to the protection of personal data concerning him or her.
> (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it ratified
> (3) Compliance with these rules shall be subject to control by an independent authority.

Like the European Union's current Data Protection Directive, the new General Data Protection Regulation (GDPR) places conditions on processing any kind of personal data. For 'lawful processing' to occur, a legal basis for the use of that data must be documented, and it cannot violate eight key individual rights, as listed below. The GDPR has specific policies for the protection of children's rights as well, requiring that children must be able to understand the privacy notices, and that online services offered for children may only process data with a guardian's consent unless they are preventative or counselling services.
Individual rights according to the GDPR include:
1. the right to be informed
2. the right of access
3. the right to rectification
4. the right to erasure
5. the right to restrict processing
6. the right to data portability
7. the right to object

[43] Ibid. Article 10
[44] Ibid. Article 10-14
[45] Privacy, Data and Technology: Human Rights Challenges in the Digital Age, *A paper issued by the New Zealand Human Rights Commission* May 2018.
[46] Supra note 11

8. rights in relation to automated decision making and profiling.

The most noteworthy difference between the current Data Protection Directive and the new GDPR is an emphasis on accountability. Not only must organisations adhere to the GDPR, but they must set up their own governance system to demonstrate adherence and keep records. While there is a list of what the records must document, there is not a certain structure of governance that must be used across the board. Performing data protection impact assessments is strongly encouraged though not required[47].

Although the Nigeria constitution does not expressly provide for right to data protection, it can be inferred from section 37[48] which provides for right to privacy. Moreover, there are various legislation and Regulations apart from this section. Some of them include;

a. Freedom of Information Act 2011. Section 14 of the Act protects personal data of individuals. It protects citizen's homes, correspondence, telephone conversation and telegraphic communications.
b. The Nigerian Communication Act 2003. By virtue of the powers conferred by the NCA on the Nigerian Communication Commission (NCC), the personal data of individuals in the telecommunication industry is protected.
c. Cybercrime (prohibition, prevention etc.) Act 2015. Here, the misuse of data for fraudulent purpose are criminalized.
d. The National Identity Management Commission Act 2007 (NIMC). Section 31 of the Act makes provision for the effective operation of the Act and its powers include collection and processing of data.

Other Regulations include;

a. National Communication Commission (Regulation of Telephone subscribers) Regulation 2011
b. Consumer Protection Framework 2016
c. Credit Reporting Act 2017
d. The National Health Act 2014.

6. Conclusion and Recommendations

Some of the problems posed by cyberspace are not really new and resulting to ancient ideas may often appear to be beneficial but are not. There is now a paradigm shift from the traditional/ conventional rights guaranteed in the various international and national treaties and conventions. In order to ensure these new sets of rights that are available offline can be claimed online as well, then international communities and National bodies need to enact binding laws and or treaties and or amend the existing fundamental rights laws and conventions to accommodate the rights available online and also incorporate the new sets of rights in the cyberspace today.

In the light of the above, it is hereby recommended as follows:

a. There is need to challenge the prevailing view that human rights are an impediment to security. Government should make a case at the international level for building in backdoors and weakening encryption in order to provide access to encrypted communications for law enforcements.
b. Companies and individuals must respect human rights and governments must hold them to account and vice-versa.
c. The new sets of rights should be protected by incorporating these rights in the various existing laws and or treaties at the National and International level. The already existing rights be modified to accommodate rights of individuals online.
d. Government officials should have minimal interference in the rights of citizens guaranteed to individuals i.e. these rights should not be politically inclined or polarized.
e. Local laws should also be modified to accommodate these rights online and create awareness by publicizing the laws and punishment available to offenders.

[47] Al Lutz et al, (May 2017) Discussion paper: Data protection, Privacy and Security for Humanitarian and Development Programs. Ed. Sherrie S. Simms. Available at http://wvi.org/health/ict4d last accessed 13th August 2018.
[48] Nigerian constitution 1999