Global Journal of Politics and Law Research

Vol.3, No.4, pp.17-30, August 2015

Published by European Centre for Research Training and Development UK (www.eajournals.org)

THE SIGNIFICANCE OF INTERNET SERVICE PROVIDERS IN NIGERIA: AN OVERVIEW OF LEGAL PERSPECTIVE

Mu'azu Abdullahi Saulawa[1*] Junaidu Bello Marshall [2] Prof. Dr. Ida. Madieha bt. Abdul Ghani Azmi[3]

1. Faculty of Law, Umaru Musa Yar'adua University, P.M.B. 2218. Katsina State, Nigeria
2. Faculty of Law, Usmanu Danfodiyo University, P. M. B 2346. Sokoto State, Nigeria
3. Ahmad Ibrahim Kulliyyah of Laws, International Islamic University, Gombak, Malaysia

ABSTRACT: *The paper focuses on the significance of Internet Service Providers (ISPs) in Nigeria with a view to ascertaining the legal and regulatory framework put in place and their consistency with international best practices. ISPs are a company that provides users and companies, corporation and government accesses to internet, creation of website and virtual hosting. ISPs used devices in the communication technology to install accesses links to internet in an area. Some of the larger ISPs operate a high-speed broadband. The paper examines ISPs as service providers to internet networks across the globe for the purpose of Information and Communication Technology (ICT). The paper adopts doctrinal methodology approach wherein the relevant data collected was analysed and the finding brought out. The findings of the paper reveals that ISPs are conducting their businesses within the legal and regulatory frameworks put in place by the government and that they are duty bound to maintain a register of customers and monitor the activities of such customers and report any suspicious activities. It further reveals that Nigeria has the basic regulatory framework in monitoring the ISPs, but needs more in other to fight cyber crimes and competes globally. Therefore, the paper recommends that there should be a strong hold relationship between the law enforcement agencies and the ISPs so as to curb the menace of cybercrime. It further recommends that main ISPs should lead and enhance the way of ensuring reliability, integrity and security of the internet as a critical infrastructure and so does the others. That as a matter of urgency, the Bills before the National Assembly relating to ISPs be enacted into law in other to complement other relevant laws and to also enable Nigeria build business trust and benefits from international investment.*

KEYWORDS: Internet Service Providers, Cyber Crime, Internet, Telecommunication

INTRODUCTION

The paper focuses on the significance of Internet Service Providers (ISPs) in Nigeria with a view to ascertaining the legal and regulatory framework put in place and their consistency with international best practices. The past two decades has been a tremendous achievement in the internet applications in all part of the societies across the globe and in Nigeria. The provisions and applications of ISPs had impacted so much in the internet and on our daily activities, fundamental rights, social interactions, economics and other relevant infrastructures. The operation of ISPs proves to be an open and free cyberspace that has promoted political, economic and social attachment worldwide; it has cracked down the

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

hindrance between countries, communities and citizens, permitting interactions and sharing of information and ideas across the globe. [1]

INTERNET SERVICE PROVIDERS (ISPS)

Internet Service Provider is a company that provides internet connections and services to individuals and organizations. It further provides access to the internet, and also provides software packages (such as browsers), email accounts and personal websites or home page. ISPs also introduces website for business and can also build websites themselves. It is a connection that covers all ISPs through network access points, public network facilities on the internet spine.[2]

ISPs come in many forms and ranges and also addresses by many names: the phone company, the cable company, the wireless company. They are the internet agents; planning, manage and overseer of resources, providing reliable connectivity and ensuring that services are fully delivered.[3]

The advancement of commercial internet services and applications supported greatly in the increase rises of commercialization of the internet. This trend was the result of several other factors as well. One of the most important factors was the introduction of personal computer (PC) and the workstation in the early 1980's-a development that in line stimulate by unmatched progress in integrated circuit technology and associated swift decline in computer prices. Another important factor was the emergence of Ethernet and other 'Local Area networks' (LANs) to link personal computers and other factors do count.[4]

The development of internet as network between the government research laboratories and participating departments of universities is astounding. By the late 1980's a process was set in place toward the public, commercial use of the internet. The limitation in respect to the usage of internet was removed by 1945 that is four (4) years of the introduction of World Wide Web.[5]

The ISPs were established in Australia in 1989[6] and the United States (US). In Brookline, Massachusetts-based the world becomes the first commercial ISP in the US. Its first Customer was served in 1989.[7]

[1] European Commission, 'Cybersecurity Strategy of European Union An open Safe and Secure Cyberspace' at the Joint Communication of the European Parliament, The Council, The European economic and Social Committee and the Committee of the Regions, High Representative of the European Union for Foreign affairs and Security Policy. Brussel, 7,2,2013, JOIN (2013), Final p, 2. Available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf. Accessed on 27/01/2015.
[2] Internet Service Providers (ISP) Encyclopaedia Britannica available at http://www.britannica.com/EBchecked/topic/746032/Internet-service-provider-ISP. Accessed on 27/01/2015.
[3] Hathaway and Savage, 'Stewardship of Cyberspace: Duties for Internet Service Providers', 2012 Cyberdialogue2012, p. 2, available at http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012_hathaway-savage.pdf. Accessed on 27/01/2015.
[4] Ibid.
[5] Ibid. further to this the World Wide Web was popularly known as WWW.
[6] Clarke, Roger. 'Origins and Nature of the Internet in Australia'. Published 29 January 2004, Retrieved 21 January 2014.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

In US, the Federal communication Commission (FCC)[8] on 23rd April 2014 is reported to be considering a new rule that will permit ISPs to offer content providers a faster track to send content, thus reversing their earlier net neutrality positions.[9] According to Susan a possible solution to net neutrality concerns may be metropolitan broadband.[10]

ISP is defines as a company that provides consumers and business access to the internet. Depending on the services offered by the internet service provider, it could be considered an information service provider, storage service provider, Internet Network Service Provider (INSP), or a combination of the three.[11]

In the early years of 1990's, the internet uses telephone services that provides voice communication through an established circuit or line by means telephone network that remain persistent during the communication session. The telephone network operated according to strict closely-controlled set of processes and technologies that provided a highly reliable service, but adopted to change slowly. This method did not have an application performing interface (API) to allow for third party access and test of telecommunication services was discouraged.[12]

Today, the internet operates in a different sphere; lengthy messages are decomposed into packets that circulate from one source to another following possible different route through the network. This is called pocket switching. The internet also provides a simple interface to communication networks that makes it easier for third parties to create innovative communication based products to connect and access the internet and providers to introduce new generation of value-added services and applications. Still, the internet and the communication services that drive on it depend on the integrity of routing and naming infrastructures. These critical tasks are essential to the proper functioning of the internet.[13]

Routing of ISP

The internet encompasses all the operation of networks. Networks include of end system, called hosts, and intermediate system called routers, connected through communication channels.[14] Information flows through a network line chosen by routing process that is established by routers. A router is a networking device that transmits data packets between computer networks. A router is connected to two or more data lines from different networks.

---

[7] Robert H'obbes' Zakon. 'Hobbes' Internet Timeline v10.1', published as Robert H. Zakon (November 1997) Retrieved November 14, 2011.

[8] The Federal Communications Commission (FCC) is an independent agency of the United States government, created by Congressional statute (see 47 U.S.C. § 151 and 47 U.S.C. § 154) to regulate interstate communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. The FCC works towards six goals in the areas of broadband, competition, the spectrum, the media, public safety and homeland security. Available at http://en.wikipedia.org/wiki/Federal_Communications_Commission. Accessed on 27/01/2015.

[9] Wyatt, Edward (23 April 2014). "F.C.C., in 'Net Neutrality' Turnaround, Plans to Allow Fast Lane". New York Times. Retrieved 2014-04-23;

[10] Professor Susan Crawford, a legal and technology expert at Harvard Law School. (28 April 2014). 'The Wire Next Time'. New York Times. Retrieved 2014-04-28.

[11] ISP (Internet Service Provider), 'Definition of ISP', Investopedia, available at http://www.investopedia.com/terms/i/isp.asp. Accessed on 27/01/2015.

[12] Hathaway and Savage, op. cit, p. 3.

[13] Ibid.

[14] Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination.[15]

Naming of ISP

The process of naming services in ISP is essential to both their customers and other internet users. Naming is referred as domain names that are human-friendly names and they translated into Internet Protocol (IP) address, for example www.gmail.com is a domain name, and 212.28.199.27 is the IP address. More often, users adopted to use domain names and routers like to use IP addresses.[16]

SIGNIFICANCE OF ISPS

The magnitude of ISP is outstanding in the application of cyberspace. ISPs are responsible for providing internet connecting and maintaining the network infrastructure. A number of ISPs provide hardware and cable internet, handle the task of installing the services in a customer home or office.[17] ISPs own and operate a critical infrastructure that facilitates the delivery of essential goods and services. They form the fundamental object of this infrastructure and have an important role in fostering security. [18]

At the time a new ISP connects to the internet it absolutely consent to certain terms concerning the transmission of pockets, sharing of routing information, resolution of domain names, reporting on the status of the internet and handling emergencies.[19] While waiting for and understand more from ISP, still not clear, but there should be an explicit duty to comply with technical aspects of internet participation. In examine the rapid development in the internet complexity and the critical role of internet has come to play in the global economy, providers should be mandated to be overseer of the global enterprise. As today we cannot take a step for a click away from an infection, disruption or worse yet, no service.[20]

In analysing the significance of ISP and finding a way forward, Professor Lillian Edwards made an emphasis on the increasing pressure from states, mainly on ISPs to guard, public morality by filtering child pornography, hate speech, racist content etc. she further argued that these pressure combined may represent a tipping point time towards more liability on internet intermediaries.[21] Lillian further shared her experience on informally gathering data on the use of notice and take down in the United Kingdom, emphasising how difficult it was

[15] Router (computing), Wikipedia, available at http://en.wikipedia.org/wiki/Router_%28computing%29. Accessed on 27/01/2015.
[16] Hathaway and Savage, op. cit, p. 3.
[17] The importance of ISPs, eHow, available at http://www.ehow.com/facts_7490930_importance-isp.html. Accessed on 27/01/2015.
[18] Hathaway and Savage, op. cit, p. 4.
[19] A network that is under the administrative control of one organization is called an autonomous system (AS). There are approximately 40,000 ASes operating today. For the purposes of this paper, we treat the acronym ISP as a synonym for either ISP or AS. Routing within an AS is called intradomain routing whereas routing between ASes is called interdomain routing.
[20] Hathaway and Savage, op. cit, p. 4.
[21] Lillian Edwards, a Professor of internet law at the University of Sheffield, in a response question by the session chair on whether there is special requirements for search engines in a 'Introduction to the Role of Internet Intermediaries in Advancing Public Policy Objectives', Workshop Summary OECD, 16 June 2010, Paris, France.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

to obtain. In addition to this, Lillian noted that ISPs have no incentive to share this data and suggested the possible need for public sector intervention.[22]

ISPs IN NIGERIA

With the development of ISPs across the globe, Nigeria took a bold step in ensuring the use of ISPs for the purpose of utilization of ICT. There are many ISPs in Nigeria and while some of them are fast, others are not so fast. Some ISPs are the main service providers while others are basically the clients of the main ISPs making them secondary ISPs.[23] Some of the internet speed tends to differs from other ISPs to another ISP and that slows down as the user deals with lower ISP, usually did this to reduce the speed so as to make profit from the main ISP which provides them with the service. The following are some of the top ISPs in Nigeria and their average:[24]

	Name of ISP	**Averages**
1	PROVIDER LIR	13.98 Mbps
2	Netcom Africa Limited	12.19 Mbps
3	Galaxy Backbone Plc	11.91 Mbps
4	Smile Communications Ltd	7.51 Mbps
5	MTN Nigeria	6.93 Mbps
6	SWIFT NETWORKS LIMITED	6.65 Mbps
7	MainOne Cable Company	5.89 Mbps
8	IPNXng	5.21 Mbps
9	VDT Communications Limited	4.80 Mbps
10	Suburban Telecom	4.73 Mbps
11	Internet Solutions Nigeria Limited	4.45 Mbps
12	SPECTRANET LIMITED	3.92 Mbps
13	NGCOM	3.61 Mbps
14	Wireless Broadband Internet service	2.64 Mbps
15	Spectranet Ltd	2.63 Mbps
16	Coollink	2.41 Mbps
17	Swifttalk Limited (NG)	2.34 Mbps
18	Mobitel Nigeria Limited	2.03 Mbps
19	EMTS Limited / Etisalat Nigeria	2.01 Mbps
20	Globacom Limited	1.86 Mbps

[22] Ibid. this is a response to the Panel discussion in respect of sharing data also noted however that some firms such as Google were making efforts to make data available.
[23] What is your fastest Internet Service Provider in Nigeria? Kolitech. Nigeria, available at www.kolitech.com/cgi-bin/page.pl?internet&bn=1&m=11. Accessed on 27/01/2015.
[24] These are the 20 fastest ISPs in Nigeria, available at www.techsurplex.com/2013/11/19/20-fastest-isps-nigeria/. Accessed on 27/01/2015.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

AN OVERVIEW OF LEGAL PERSPECTIVE

The discussion on the legal perspective premise on analysing some of the relevant laws that dealing with ISPs as in Council of Europe Cybercrime Convention, Nigerian legislations and guidelines.

Council of Europe Cybercrime Convention

The Convention was opened for signature in Budapest, on November 23, 2001.[25] Thirty-five countries have signed the treaty, with Albania and Croatia having ratified it as well.[26] The Convention will come into force when five states, three of which must be COE members, have ratified it.[27] The treaty is intended to create a common cross-border "criminal policy aimed at the protection of society against cybercrime ... by adopting appropriate legislation and fostering international co-operation."[28] Our discussion on the Convention will now be narrowed to some salient Articles that deal with ISPs.

Article 1, primarily defines four fundamental terms to the Convention. These terms defines the critical infrastructural position focused by the Convention. It first defines:

> 'computer system' means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; [29]
>
> 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;[30]
>
> 'service provider' means: [31]
>
> i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
>
> ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service;
>
> 'traffic data' means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of

[25] The Convention, Many of the crimes committed against individuals and businesses are legislated against in the European Convention on Cybercrime, and include identity theft, child pornography, and fraud, among others. Convention on Cybercrime opened for signature Nov. 23, 2001, Europ.
T.S. No. 185 [herein after Convention], available at http://conventions.coe .int/ Treaty/EN/ projets/FinalCybercrim e.htm (last visited Dec. 4, 200 2).
[26] Ibid.
[27] Wendy McAuliffe, Council of Europe Approves Cybercrime Treaty, ZDNET UK NEWS (Sept. 2 1, 2001), at http://new s.zdnet.co.uk/sto ry/0,,t269 -s2095796,00 .html
[28] The Convention, Op. cit, preamble.
[29] Article 1 (a) Ibid.
[30] Article 1 (b), Ibid.
[31] Article 1 (c), Ibid

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

> communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.[32]

Article 11 highlights on Attempt and Aiding or abetting, it provides that in establishing these offenses 'the commission of the offenses defined in the Convention.'[33] Liability under this Article arises when "the person who commits a crime established in the Convention is aided by another who also intends that the crime be committed."[34] For example, the transmission of a virus is an act that sparks the operation of a number of articles of the Convention. However, transmission can only take place through an ISP. 'A service provider that does not have the requisite criminal focused cannot incur liability under this section."[35] Therefore, there is no duty under this section for an ISP to actively monitor content in order to avoid criminal liability under this section.[36]

Analytically, it is morally and ethically right if ISPs in the course of their operations monitor or cite and a beep comes up in their mainframe indicating an imminent danger of attacker to notify the respective bodies like the law enforcement agencies. Implementing this action will certainly prevent a lot of cyber-attacks and cyber related offences perpetrated in our communities instead of knowing that the cybercrime is on-going and decided to hold on till it becomes a threat to the individual, society or national security.

Article 16 discusses Expedited Preservation of Stored Computer Data which relates to the expedited preservation of stored computer data, that a new approach be instrumented so as to simplify the investigation of cybercrimes.[37] This Article applies only to data that has already been collected and retained by ISPs.[38] One must not confuse "data preservation" with "data retention."[39] For purposes of analysing this Article, data retention merely relates to the protection from deterioration of data already existing in stored form.[40]

Article 17 cite the Expedited Preservation and Partial Disclosure of Traffic Data and further provide that:

> to ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; [41]and ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.[42]

---

[32] Article 1 (c), Ibid.
[33] Ibid.
[34] Ibid.
[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Explanatory Report of the Com m. of Ministers [of the Convention n on Cybercrime], 109th Sess. (adopted on Nov. 8 , 2001), art. 1(a), 23 [hereinafter Explanatory Report] (on file with the Journal of Transnational Law & Policy).
[39] Ibid.
[40] Ibid.
[41] Article 17 (1) (a), Ibid.
[42] Article 17 (1) (b), Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

If preservation of 'traffic data' as contained under Article 16 will be facilitated accordingly and the immediate disclosure of some 'traffic data', the authorities can identify the person or persons who have distributed the object for instance child pornography or computer viruses.[43]

The importance of this Article considering the above example, it defines frequently several service provider is involved in the transmission of a communication. Every single service provider may possess some 'traffic data' related to the transmission of the detailed communication, which either has been produced and engaged by that service provider in relation to the [actual] passage of the communication amid its system or has been provided by other ISPs.[44] For business-related, security or technical purposes, sometimes 'traffic data' is shared among the service providers involved. [45]

Article 18 relates to production orders and further provides that:

> a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; [46] and a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.[47]

The Article explicitly allow 'competent authorities to compel a person in its territory to provide specified stored computer data' or to compel an ISP to provide subscriber information. [48] In addition it exclusively relates to production of stored or existing data, not 'traffic data' or 'content data related to future communications'.[49] The processes of production orders precede search and seizure as a means of obtaining specific data.[50]

Article 20 provides for real-time collection of traffic data and further discusses:

> collect or record through the application of technical means on the territory of that Party, [51] and compel a service provider, within its existing technical capability: [52]
>
> to collect or record through the application of technical means on the territory of that Party; [53] or to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. [54]

Focusing on the importance of collecting 'traffic data' in order to determine the origin, sources or destination of the cybercrime being committed is essential. For this reason, ISPs

[43] Ibid. Explanatory Report, op. cit, at 165-166.
[44] Ibid.
[45] Ibid.
[46] Article 18 (a), Ibid.
[47] Article 18 (b), Ibid.
[48] Ibid. Explanatory Report, op. cit at 170
[49] Ibid.
[50] Ibid. at 175.
[51] Article 20 (1), (a), Ibid.
[52] Article 20 (1), (b), Ibid.
[53] Article 20 (1), (b), (i), Ibid.
[54] Article 20 (1), (b), (ii), Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

familiar about the interception must be under obligatory to maintain complete confidentiality in order for this to be successful.[55]

Advance Fee Fraud and other Fraud Related Offences Act 2006

In Nigeria, the only law that directly controls the issue of ISPs is the Advance Fee Fraud and other Related Offences Act 2006 (AFROA), which for all intents and purposes made Nigeria, regulates the ISPs in line with international practices. Through failure of the National Assembly to pass other related Bills in to law would greatly affect the impact of the AFROA in combating cyber crimes in Nigeria.

Part II of the AFROA deals with Electronic Telecommunication Offences and provides in Section 12 thus:

‘’12 (1) Any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form shall be required to obtain from the customer or subscriber:

(a) full name;

(b) residential address, in the case of individual

(c) corporate address, in the case of corporate bodies

(2) Any customer or subscriber who-

(a) fails to furnish, the information specified in subsection (1) of this section; or

(b) with the intent to deceive, supplies false information or conceals or disguises the information required under this section, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or a fine of N 100,000.

(3) Any person or entity providing the electronic communication service or remote computing service either by e-mail or any other form, who fails to comply with the provisions of subsection (1) of this section, commits an offence and is liable on conviction to a fine of N100,000 and forfeiture of the equipment or facility used in providing the service.

(1) Notwithstanding the provisions of the Nigerian Communications Act 2003 or the provisions of any other law or enactment, any person or entity who in the normal course of business provides telecommunications or internet services or is the owner or person in the management of any premises being used as a telephone or internet cafe or by whatever name called shall-

(a) be registered with Economic and Financial Crimes Commission (in this Act referred to as ‘’the Commission’’);

(b) maintain a register of all fixed line customers which shall be liable to inspection by any authorized officer of the Commission; and submit returns to the Commission on demand on the use of its facilities.

[55] Ibid. Explanatory Report, op. cit. at 225

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

(2) Any person whose normal course of business involves the provision of non-fixed line or Global System of Mobile Communications (GSM) or is in the management of any such services, shall submit on demand to the Commission such data and information as are necessary or expedient for giving full effect to the performance of the functions of the Commission under this Act.

(3) Any person specified under subsection (1) and (2) of this section shall exercise the duty of care to ensure that his services and facilities are not utilized for unlawful activities.

(4) It shall be a valid defence for any provider of wire or electronic communication service, its officers, employees or agents or other specified persons for providing information or facilities to the Commission in any cause, matter or suit that the said provider, its officers, employees or agents or any other specified persons acted in compliance with the obligations imposed under this Act''.

The above mentioned provisions of AFROA dealt with ISPs statutory requirements to register with Economic and Financial Crimes Commission (EFCC) and to also maintain a register of their customers which contains the name and addresses of all the customers and to toward same to EFCC officials when the officials demand same.

It further provides that a person or service provider, body corporate who wilfully contravenes the provisions of this section commits an offence and shall be liable on conviction to a fine of not less than N100,000 or imprisonment for a term not less than 3 years or both fine and imprisonment.

AFROA further provides protection to any service provider, its officers, its employees or duly authorized agents may, in the normal course of work, carry out the activity mentioned in the above provisions of AFROA.

The discussion of this section is on the ISP and they are the major stakeholders in the used of internet and will provide a great contribution in tackling the menace of cyber attack. Without incorporating the Service providers, the objective of the legislation would be defeated.

Nigerian Communications Act 2003 [56]

The opening chapter of the Act discusses objectives, application and scope.[57] The primary object of this Act is to create and provide a regulatory framework for the Nigerian communications industry and all matters related thereto and for that purpose and without detracting from the generality of the foregoing, specifically to—[58]

promote the implementation of the national communications or, telecommunications policy as may from time to time be modified and amended;[59]

establish a regulatory framework for the Nigerian communications industry and for this purpose to create an effective, impartial and independent regulatory authority;[60]

[56] The Federal Government of Nigeria Official Gazette, No 62, Vol. 90, 19th August 2003, Lagos, Printed and Published by The Federal Government Printer, Lagos, Nigeria. FGP 173/82003/2,000 (OL 77).
[57] Chapter I, Ibid.
[58] Section 1 of the Act, discuss objectives, Ibid.
[59] Section 1 (a), Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

promote the, provision of modem, universal, efficient, reliable, affordable and easily accessible communications services and the widest range thereof throughout Nigeria;[61]

encourage local and foreign investments in the Nigerian communications industry and the introduction of innovative services and practices in the industry in accordance with international best practices and trends;[62]

ensure fair competition ill all sectors of the Nigerian communications industry and also encourage participation of Nigerians in the ownership, control and management of communications companies and organisations;[63]

encourage the development of a communications manufacturing and supply sector within the Nigerian economy and also encourage effective research and development efforts by all communications industry practitioners;[64]

protect the rights and interest of service providers and consumers within Nigeria;[65]

ensure that the needs of the disabled and elderly persons are taken into consideration in the provision of communications services ;[66] and

ensure an efficient management including planning, coordination, allocation, assignment, registration, monitoring and use of scarce national resources in the communications sub-sector, including but not limited to frequency spectrum, numbers and electronic addresses, and also promote and safeguard national interests, safety and security in the use of the said scarce national resources. [67]

It further provides that this Act applies to the provision and use of all communications services and networks, in whole or in part within Nigeria or on a ship or aircraft registered in Nigeria.[68]

The Act provides that the Commission may also make and publish guidelines on any matter for which this Act makes express provision and such other matters as are necessary for giving full effect to the provisions of this Act and for their due administration.[69] In addition to this provision, that the Nigerian Communications Commission issue a guidelines to ISPs.

[60] Section 1 (b), Ibid.
[61] Section 1 (c), Ibid.
[62] Section 1 (d), Ibid.
[63] Section 1 (e), Ibid.
[64] Section 1 (f), Ibid.
[65] Section 1 (g), Ibid.
[66] Section 1 (h), Ibid.
[67] Section 1 (i), Ibid.
[68] Section 2 of the Act discusses application and scope, Ibid.
[69] Section 70 (2) of the Act, Part VI discusses regulations and guidelines etc. Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission.

These Guidelines apply to all licensees providing Internet access services or any other Internet Protocol based telecommunications services (hereinafter, "ISPs"). [70]

The guidelines provide that all ISPs shall comply with the Consumer Code of Practice Regulations, 2006.[71] For greater certainty, in the event that any ISP, including by participation in an association of ISPs, does not submit an individual consumer code pursuant to Regulation 10 of those Regulations, the provision of services and consumer practices applicable to that ISP shall be governed by the General Code attached as Schedule 1 to the Regulations.[72] Also in addition to the information disclosure requirements described in Part II of the General Code, ISPs shall ensure that they disclose the following information regarding their provision of Internet access services: [73].

ISPs must make full and fair disclosure of information regarding bandwidth (including whether bandwidth is shared or dedicated to the user) and bit transfer rates to Consumers before the process of subscription is concluded;[74] ISPs must give their subscribers notice of any planned upgrade of ISP equipment, which could have any material effect on continuing use of the services, at least six (6) months before making the change;[75] ISPs must give their subscribers notice of any winding- up or other discontinuation of the services at least six (6) months before such discontinuation;[76] and ISPs must maintain an up-to-date list of their subscribers, particularly commercial subscribers such as cybercafés or other resellers to which they provide service.[77]

The guideline further provides that in complying with the Consumer complaints provisions of Part VII of the General Code, ISPs shall ensure:[78] that they maintain one or more customer care centres dedicated to handling complaints arising from the use of their services; [79] and that efficient procedures for lodging complaints are clearly described, including the timing for the ISP's initial response and anticipated timeline for complaint resolution.[80]

The guidelines provide that the ISPs must Response to Inappropriate or Illegal Use,[81] and also it provides for the Cooperation with Enforcement Agencies.[82] That the ISPs must include a provision for Termination of Service Agreements,[83] and further provides that the ISPs must have records and data retention.[84]

[70] Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission.
[71] Part I on compliance with general consumer code of practice Section 1, Ibid.
[72] Section 2, Ibid.
[73] Section 3, Ibid.
[74] Section 3, (a), Ibid.
[75] Section 3, (b), Ibid.
[76] Section 3, (c), Ibid.
[77] Section 3, (d), Ibid.
[78] Section 4, Ibid.
[79] Section 4, (a), Ibid.
[80] Section 4 (b), Ibid.
[81] Part II on investigation and enforcement, Section 5, Ibid.
[82] Section 6, Ibid.
[83] Section 7, Ibid.
[84] Section 8, Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

It further provides that the ISPs must ensure the protection of end user,[85] and provides for additional protection of minors.[86] And that the liability of ISPs as content intermediaries,[87] and provides for takedown notices where ISPs must have in place a procedure for receiving and promptly responding to content related complaints, including any notice to withdraw or disable access to identified content issued by the Commission or other legal authority ('takedown notices').[88]

The above mentioned legislations and regulatory guidelines in Nigeria are said to be of great significance in regulating ISPs in Nigeria, but failure of the National Assembly to pass into law several Bills pending before it including the Cyber Security and Protection Agency (Establishment, etc) 2008, which intends to register and monitor the activities of ISPs indicates that much is desired in the area of regulation.

FINDINGS

The finding of the paper reveals that ISPs are the major providers that collectively have unparrarelled access into global networks, which enables the ISPs to use their tools properly to detect cyber intrusion and attacks. The paper also reveals that without ISPs, networks cannot operate and interconnect. ISPs are the most viable devices in the ICT. The paper further finds that in Nigeria that some ISPs are faster and stronger than others, although there are primary and secondary ISPs, the primaries are the main service providers to the secondary. There are agitations that some ISPs operate this saga to slow the speed and service providers so as to make money. In this context some ISPs limits the spread of spam, notify customers of botnet infection and partner with law enforcement to deny circulations of child pornography. In addition to this, the paper reveals that ISPs are the most instrumentally connected networks that will assist in collection of data, internet protocol and provides a 24 hours a week uninterrupted services. If nations will come together to make a strong unity in defining the codes of conduct for ISPs to adopt that will yield a more secure internet infrastructure and service.

Finally the paper revealed that Nigeria has the basic legislations on the ISPs regulation like its counter parts in the world and that there are important Bills pending before the National Assembly, which will add value to Nigeria's effort in a fight against cyber crimes and related offences.

CONCLUSION AND RECOMMENDATIONS

Internet presents a critical infrastructure in its application and other forms surrounds it hold the future. Its application covers both economic, defence and social activity across the globe. ISPs present an enormous responsibility in sharing, connecting and managing of networks in the internet. The ISPs have duty to provide networks across the globe and to provide reliable and accessible channel of services. ISPs fundamentally provides for a routing information

[85] Part III on content related activities, section 9, Ibid.
[86] Section 10, Ibid.
[87] Section 11, Ibid.
[88] Section 12, Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

and authentic and authority naming infrastructure, it proves that the networks are platform on which internet users rely should not be vulnerable to operator error or cyber-attack. Users will not accept a situation where a simple click will lead to an infection of virus or no service and that is why the legislators are to be serious in passing pending Bills into Acts so as to abridge the situation.

Therefore, the paper recommends that there should be a strong hold relationship between the law enforcement agencies and the ISPs so as to curb the menace of cybercrime. Also the main ISPs should lead and enhance the way of ensuring reliability, integrity and security of the internet as a critical infrastructure and so does the others. That as a matter of urgency, the Bills before the National Assembly relating to ISPs be enacted into law in other to complement other relevant laws and to also enable Nigeria build business trust and benefits from international investment.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)