4. Conclusion

The internet is a landmark innovation created by humanity, the avenues of crimes committed by this creation has superseded humanity. The internet has enhanced education, communication, transportation, information and technology. With these advantages comes the increase in cybercrime. The effect of cybercrime is crippling Nigeria's image, progress and consumers' trust in the internet. There is an urgent need to sanitize the cyberspace. This paper examined the role of ISPs in Nigeria and found it inadequate to police and secure the cyberspace. Lessons can be learnt from the Budapest Convention on Cybercrime and the E-Commerce Directive. The guidelines make provisions on how law enforcement agencies and ISPs can structure interaction that would help tackle the cybercrime phenomenon. While the directive's Articles 12 to 15 stipulate liabilities for online intermediaries. The lessons drawn from these international instruments can help in the fight against cybercrime. Combating and investigating cybercrime is an extremely complex task. It would entail legal strategies and technical measures. The Nigerian legislature should amend the Cybercrime Act and extend the duties of ISPs to include monitoring activities under their watch and block access when legally necessary. ISPs possess the technical expertise to monitor and block access of illegal activities. The investigation and prosecution of cybercrime will be more efficient when ISPs and law enforcement agencies work hand in hand in an efficient manner. The joint effort of both sectors would enhance a safer internet ecosystem if they respect their distinct roles and avoid encroaching on the rights of internet users. A legislative framework that clearly defines the duties and limitations of ISPs and law enforcement agencies in the fight of cybercrime would yield greater results.

unauthorized or illegal activities, they should use these infrastructures to stop the commission of cybercrimes and enhance cybersecurity. The CCPA should be reviewed and amended to expand the duties of ISPs to include monitoring and policing the cyberspace

This paper argues that there are gaps in the CCPA. There is no section in the Act that addresses the implementation of the law. No institution or agency was created to enforce the specific laws created in the CCPA. The Cybercrime Advisory Council is a policy making body under the CCPA. However, the Act did not bestow on the body the power to implement the laws created in the CCPA. The implementation and enforcement of laws is a peculiar problem in Nigeria. The CCPA should be amended to address this lacuna of enforcement.

4.3. Lessons for Nigeria

Lessons should be learnt from the E-Commerce Directive which provided a harmonised liability on online intermediaries. Nigerian courts should take a cue from their European counterparts that are willing to find that ISPs have a duty of care in some circumstances to secure the network of their subscribers. The decision in *LICRA v Yahoo*[89] shows that it is technically feasible for ISPs to monitor and block illegal activities. This paper submits that ISPs should be vested with monitoring responsibilities. However, this responsibility should be carried out accurately, confidentially and without breaching the privacy rights of consumers. The private information of subscribers obtained in such process should be guarded jealously. ISPs will be held accountable for all information they come across. The duties of ISPs in Nigeria should include the notice and take-down scheme. Once an ISP is notified of an illegal activity online, it should take-down such content and block access.

---

89 Supra, (n 65).

the time being, responsible for the regulation of communication services in Nigeria, for a period of 2 years.

(2) A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section or any law enforcement agency-

(a) Preserve, hold or retain any traffic data, subscriber information, non- content information, and content data; or

(b) Release any information required to be kept under subsection (1) of this section…

In summary, the Act mandates that service providers shall keep traffic data and subscriber information for a period of 2 years bearing in mind the individual's constitutional right to privacy and employ due diligence to safeguard the confidentiality of the data retained, processed or retrieved. This provision is somewhat similar to Article 14 of the Budapest Convention although section 38 is wider because it includes the obligation to collate data. Article 14 only requires Parties' to take measures to enable the competent authorities to order or obtain the expeditious preservation of specified computer data, including traffic data. However, the scope of section 38 is limited to just service providers unlike the European E-Commerce Directive regime which affects not just ISPs but also ISSPs. This paper argues that the duties provided by the Cybercrime Act, 2015 is insufficient to ensure the reliable delivery of an essential service. ISPs should be capable guardians to their subscribers.

From the wordings of section 38, there is no legal duty placed on ISPs to secure the network for consumers. There is no specific law in Nigeria obligating ISPs to check the material or activities of their subscribers. It is arguable that ISPs have the requisite infrastructure to uncover illegal activities carried out by subscribers registered under them. They possess the technical know-how to monitor contents and activities carried out under their services. Since they have this expertise to monitor and block

different statutes and has different legal sanctions. For instance, section 419 of the Criminal Code provides that 'any person who by false pretence, and with the intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years…'. While under the Advance Fee Fraud Act,[86] the penalty on conviction for committing any of the false pretences offence is imprisonment for a term of not less than seven years without the option of a fine, or imprisonment for a term of not more than twenty years.

Ibekwe and Nwafor argue that internet fraud differs from municipal and basic fraud.[87] They stated that 'it would have been expected that the Cybercrime Act would have repealed existing laws, but it did not'.[88]This paper agrees with this line of argument. The existence and diversity of autonomous legislation as regards cybercrime amounts to cyber-pluralism and it causes confusion rather than curbing cybercrime.

The CCPA provides amongst other things the duties of ISPs and the punishments to be meted out upon failure to perform those duties. Section 38 of the CCPA, 2015 states the duties of service providers as:

(1) A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for

---

[86] Advanced Fee Fraud and other Fraud Related Offences Act 2006, s 1.

[87] They stated that the crimes related to internet fraud consist of basic ingredients of the municipal fraud offences and also input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing, with financial and personal benefits as the underlying motivation.

[88] Ibekwe and Nwafor, (n 84).

against cyber threats and attacks.[82]The Cybercrime Act, 2015 is the first cyber-specific Act to provide for the prohibition, prevention, detection, investigation and prosecution of cybercrimes in Nigeria. Before it came into existence, there was a lot of outcry for a cyber-specific law with the effect of mitigating and punishing cybercrimes in Nigeria.

It is important to note that there are other legislative frameworks that have the responsibility of detecting, investigating and prosecuting computer related offences in Nigeria. These frameworks include the Criminal Code Act 1990; Penal Code Law; Advanced Fee Fraud and Related Offences Act 2000; Economic and Financial Crimes Commission Act 2004; the Corrupt Practices and other Related Offences Act 2000 and the Money Laundering (Prohibition) Act 2011. The existence of these laws and the CCPA can be described as pluralism in the Nigerian cybercriminal law.[83]The cyber-plural system in Nigeria simply means that there exist diverse and autonomous legal orders within a legal system.[84]The existence of different laws with the objective of detecting and prosecuting fraud or cybercrime leads to conflicts of which law should be applied in prosecuting cyber-related offences. This multiplicity of laws leads to the confusion of which applicable law should be used where an accused person commits an online fraud.[85] The issue of what punishment would be meted out to the accused would also arise where a similar act is an offence in

---

82 Adedeji Adekunle, 'A Review of the Cybercrime Act 2015' Adedeji Adekunle (ed), *Combatting Cybercrimes in Nigeria: Trends and Issues* (Abuja: NIALS Press 2017) 1.

83 Nigerian legal pluralism is as a result of the fact that laws in Nigeria are derived from three distinct legal systems. The customary law, Islamic law and English style laws. Legal pluralism is prevalent in former colonies, where the law of an erstwhile colonial authority may exist alongside traditional legal systems.

84 Chibuko R Ibekwe, NA Nwafor & Anor, 'The Nigerian Cyber-Pluralism Experience' [2016] *NSU-PBLJ.*

85 Ibid.

3.3. The African Union on Cyber Security and Personal Data Protection 2014

Nigeria is also a signatory to the African Union on Cyber Security and Personal Data Protection. This Convention was adopted in 2014 with the goal of addressing the need for a harmonized legislation in the area of cyber security amongst member States of the African Union. The Convention seeks, with respect to substantive criminal law, to modernise instruments for the repression of cybercrime.[79] The Convention intensifies international cooperation. It provides that State Parties shall ensure the legislations and/or regulations adopted to fight cybercrime will strengthen the possibility of regional harmonization of these legislative measures and respect the principle of double criminal liability.[80]The Convention also specifies the promotion of exchange of information and the efficient sharing of data on bilateral and multilateral basis.[81]

Regardless of its commendable provisions, there is no provision in the Convention that encourages Member States to take necessary legislative measure to ensure that ISPs monitors activities under their watch. This paper submits that the role of ISPs is an important aspect that can enhance cyber security if proper legislative and enforcement measures are created. It should not be ignored by regional or international legislation.

3.4. The Cybercrime (Prohibition Prevention etc) Act, 2015

The Cybercrime (Protection and Prohibition) Act (CPPA), 2015 provides legal bases for the investigation and prosecution of cybercrimes. It also prescribes a proactive and response strategy

---

79 PT Akper and Adejoke O Adediran, 'Cybercrimes and the International Legal Order' in Adedeji Adekunle (ed), *Combatting Cybercrimes in Nigeria: Trends and Issues* (Abuja: NIALS Press 2017) 23.

80 Ibid. See Article 28.

81 Ibid. See Article 28(2).

By about the year 2000, a rough consensus had emerged in both Europe and the US that ISPs should in principle be left free from liability for content authored by third parties, so long as they were prepared to co-operate when asked to remove or block access to identified illegal or infringing content.[76]

This paper is of the view that the freedom of ISPs from full liability of content authored by third parties is a negation of the duties expected from ISPs from their customers. It is equitable for ISPs to use their stance in the ecosystem to detect cyber-attacks as they are forming and address them immediately by informing the victim and blocking access of the cyber-criminal.

3.2. Economic Community of West African States (ECOWAS) Directive on Cybercrime 2010

Ecowas is a regional group of fifteen countries[77] with the mission to promote economic integration of its member states. The ECOWAS Directive on Cybercrime was adopted by ECOWAS with the paramount aim of conforming the substantive criminal law and the implementation procedure of member states to tackle the cybercrime issue. Nigeria is a signatory of the Directive and has ratified it with the enactment of the Cybercrime Act.[78]The Directive does not address the issue of duties of ISPs, it concentrated more on the substantive criminal law.

---

[76] Ibid.

[77] Consisting of Benin, Burkina Faso, Cape Verde, Ivory Coast, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

[78] Chibuko R Ibekwe and NA Nwafor 'Matters Arising from Nigerian Cybercrime Act 2015- A Case for Interim Legal Transplant' [2016] (2)(3) *COPIL Journal*.

can play in enhancing cyber security. They have the ability to block access to the internet whenever they notice an illegal activity online.

The second factor ISPs raised is that they are mere messengers not content providers and thus that it would be inequitable to hold them liable.[70] Finally, the fledging European ISP industry argued that their emergent business could not withstand the burden of full liability for content authored by others.[71] Since the promotion of e-commerce and information society in Europe depended on a reliable and expanding internet infrastructure, an immunity regime was in the public interest.[72] Without it, the ISP industry had not yet been absorbed into the concentrated market of cross-media conglomerations that now dominate the modern internet services market.[73]

From the mid-1990s, in the United States and the United Kingdom, ISPs made largely successful claims that they should be exempted from liability on the basis of some kind of innocent dissemination defence, a term borrowed from the law of defamation.[74] In the United States, the DMCA resulted in a series of safe harbours. Against this plea in Europe, however, was the Commission's strong belief that ISPs, as only effective gatekeepers, should take on the role of cleaning up the internet that is, ridding it of pornography, spam, libel and other forms of undesirable contents.[75] This was a policy goal to ensure child protection and to boost public trust and confidence in the internet as a safe space for economic activity. It is submitted that since it was conceivable for ISPs to clean up the internet, it is equally possible for them to police the cyberspace and enhance cybersecurity.

---

70 Edwards, (n 61).
71 Ibid.
72 Ibid.
73 Ibid.
74 Ibid.
75 Ibid.

carry no liability for content carried but do owe duties of confidentiality.[68]

There are two limbs to the above argument. Firstly, the amount of delay and expense that would be incurred if they manually check the legality of materials that pass through their services. Secondly, the invasion of consumers' privacy and confidentiality. It is arguable that checking materials within their services is conceivable. The security of subscribers should be of paramount importance to all ISPs. The delay or expense that would be incurred whilst seeking such security would be worth the safety of the cyberspace.

The possibility of an ISP checking the legality of materials was upheld in *France v Yahoo* case (*LICRA v Yahoo*).[69] In this case, LICRA complained that Yahoo! allowed their online auction service to be used for the sale of memorabilia from the Nazi period, contrary to Article R645-1 of the French Criminal Code. The defence rested on the fact that these auctions were conducted under the jurisdiction of the United States. The court ordered Yahoo to take all appropriate measures to deter and prevent access to auctions of Nazi memorabilia on its site by French residents. Yahoo contended that it was impossible to comply with this order. The report of the court-appointed experts noted that, as of 2000, roughly 70% of French internet users could be identified as such by the DNS database. The report showed that, in fact, Yahoo had the capacity to identify and thus block access to 90 per cent of French citizens. Accordingly, Yahoo was instructed to block access.

It is obvious from the court's decision and report of the court appointed experts that ISPs can check materials that pass under their watch. This case offers insights on the crucial role ISPs

---

[68] Ibid.

[69] *Tribunal de Grande Instance de Paris* (Superior Court of Paris) 22 May 2000.

ISPs quickly became aware of their potential high-risk status in content liability cases sometime in the early to mid 1990s'.[61] As a result of this, ISPs pleaded a case for immunity from content liability around the world.[62] This heavily informed the development of limited liability regimes in the United States Digital Millennium Copyright Act (US DMCA)[63] and the ECD. The ISP plea rested mainly on three factors: lack of effective legal or actual control, the inequity of imposing liability upon a mere intermediary (shooting the messenger), and in Europe especially, consequences for the public interest if unlimited liability was, nonetheless, imposed.[64] It is important to discuss the three factors raised by the ISPs.

On the first point, ISPs argued that they could not possibly check manually, the legality of all the materials which passed through their servers, without impossible amounts of delay and expense.[65]They also argued that it is not possibly legal for them to do so without invading the privacy and confidentiality of their subscribers.[66] Their aim was to be classified legally not as publishers who carried the risk of content they made available to the public but as common carriers.[67]A classification that is akin to the postal service and telephone companies in the US, institutions that

---

61 Lilian Edwards, 'The Fall and Rise of Intermediary Liability Online' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet,* (3rd edn, Oregon: Hart Publishing 2009) 58.

62 Ibid.

63 The Digital Millennium Copyright Act (DMCA) is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). The DMCA's principal innovation in the field of copyright is the exemption from direct and indirect liability of internet service providers and other intermediaries. This exemption was adopted by the European Union in the Electronic Commerce Directive 2000.

64 Ibid.

65 Edwards, (n 61).

66 Ibid.

67 Ibid.

3.1. The European E-Commerce Directive Regime

The Electronic Commerce Directive, adopted in 2000, sets up an Internal Market framework for electronic commerce. It establishes harmonised rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers.[58] The E-Commerce Directive (ECD) Regulations 2002 implement Articles 3, 5, 6, 7(1), 10 to 14, 18(2) and 20 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services. In particular electronic commerce, in the internal Market (the 'Directive on Electronic Commerce').[59] Articles 12 to 15 of the Electronic Commerce Directive ECD introduced throughout Europe, a harmonised regime on the liability of online intermediaries.[60] The regime affects not just ISPs but also Information Society Services Providers (ISSPs). Predominantly, the ECD intermediary service provider liability regime, covers not only the traditional ISP sector, it covers also a wider range of actors who are involved in selling goods or services online, offering online information or search tools for revenue (or not); and pure telecommunications, cable and mobile communications companies offering network access services. The ECD takes a horizontal approach to ISP liability. It deals with all kinds of content issues- intellectual property, criminal obscenity, libel and so on- rather than focussing on a single area, as the US DMCA does with copyright. The ECD approach is broader and covers a variety of actors in the cyberspace.

Edwards argues that 'by virtue of their obvious role as gatekeepers to internet publication, the emerging industry sector of

---

58 'Electronic Commerce Directive' <*http://www.en.m.wikipedia.org*> accessed 20 November 2017.

59 'The Electronic Commerce (EC Directive) Regulations 2002' [11 June 2011] <*http://www.eradar.eu*> accessed 20 November 2017.

60 ISPs are intermediaries. They are viewed as the critical control points.

therefore recommended that States adopt regulations in their national law in order to fully implement the procedural provisions of the Convention on Cybercrime. It is also important to define investigative authorities and obligations of law enforcement agencies while putting in place conditions and safeguards as foreseen in Article 15 of the Convention.[56]

The guidelines provided amongst other things, Measures to be taken by Service Providers. It requires service providers to cooperate with law enforcement authorities to minimize use of services for illegal purposes. Service providers should be encouraged to report criminal incidents affecting the ISP of which he is aware of, to the law enforcement agencies. The second principal part of the Convention requires Parties to enact certain procedural mechanisms and procedures to facilitate the investigation of cybercrimes or any crime committed with a computer or for which evidence may be found in electronic form.[57]

In summary, these guidelines intend to provide strategies to secure the cyberspace without encroaching on the fundamental human rights of their customers. It tries to create a balance between subscribers' right to privacy and the cyber security strategy canvassed in the guidelines. This guideline is similar to the Cybercrime Act, 2015 of Nigeria. There is nowhere in the guideline where ISPs are to be held liable for criminal activities carried out with their network. This is only a guideline and State parties are not obliged to adopt it. This paper submits that the guidelines has not addressed the gap of ISPs duties and liability for aiding and abetting criminal activities carried out under their guardianship.

---

56 Ibid.

57 Michael A Vatis, 'The Council of Europe Convention on Cybercrime' *<http://www.static.cs.brown.edu>* accessed 22 November 2017.

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

The above provision encourages State Parties to adopt legislative measures that would criminalise the intentional use of another's computer without permission.

A guideline for the Cooperation between Law Enforcement and ISPs against Cybercrime was adopted by the Global Conference Cooperation against Cybercrime Council of Europe, Strasbourg on 1-2 April, 2008.[53] The guidelines are a non- binding tool that can now be disseminated and used to help law enforcement agencies and service providers in any country around the world. It would help organise their cooperation against cybercrime while respecting each other's roles and responsibilities as well as the rights of internet users.[54]

The objective of the guidelines is to help law enforcement authorities and ISPs, structure their interactions in relation to cybercrime issues. The guidelines are not intended to substitute existing legal instrument but assume that legal instruments exist that provide a well-balanced system of investigation instruments.[55] It is important that such instrument safeguards fundamental human rights such as freedom of expression, the respect for private life, home and correspondence and the right to data protection. It is

---

53 'Project on Cybercrime' [2 April 2008] <*http:/ www.coe.int/ cybercrime. com*> accessed 30 October 2017. These guidelines are the result of several rounds of discussions with representatives from industry and law enforcement who met between October 2007 and February 2008 under the auspices of the Council of Europe's project on Cybercrime.

54 Ibid.

55 Ibid.

blind eye to criminal activities in the cyberspace and fails to abate the cybercrime by blocking the user's IP address and notifying the police, that ISP should be liable for aiding and abetting cybercrime.

4. Duties of Internet Service Providers in other Jurisdictions

4.1. The Convention on Cybercrime

The Convention on Cybercrime,[49] is the first international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.[50] It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer States Canada, Japan, South Africa and the United States.[51] Article 1 of the Convention defines service providers as:

i. any public or private entity that provides to users of its services, 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.[52]

Chapter II of the Convention provides 'Measures to be taken at the National Level'. Section 1 covers Substantive Criminal Law. Title 1 states offences against the confidentiality, integrity and availability of computer data and systems. Article 2 covers illegal access, it provides thus:

---

49 Also known as the Budapest Convention on Cybercrime or the Budapest Convention.

50 'Convention on Cybercrime' <*http:/www.en.m.wikipedia.org*> accessed 30 October 2017.

51 Ibid.

52 2001, Council of Europe Convention on Cybercrime, Budapest, Article 1(c).

nature.[43] Most companies have purchased blocks of IP addresses that they use on a regular basis.[44] These companies may be using a combination of intranet networking,[45] which refers to computer connections in the same organization, and internet networking, which refers to computer connections from around the world. Many computers on the network may keep the same IP address to simplify networking throughout the company.[46]

Since the IP address enables the ISP to locate subscribers when they are online, it is right to say that the IP address is a dominant strategy by which cyber criminals can be tracked by the ISPs. Once the ISP notices illegal activity online, the next step should be to locate the IP address. Once this is located, the next action should be to ascertain who owns the IP address and a crime can be abated by blocking such address or notifying the police of the illegal activity.

The general belief is that the main duty of ISPs is to provide internet access to its customers. According to Eeten et al,[47] the ISPs customers can only access, send and receive traffic via the ISP. He opines that this creates a natural bottleneck to mitigate malicious activity of the customers' machines.[48]This paper argues that the main duty of ISPs is to back up the provision of internet access to customers with adequate security. The law should provide the duties of ISPs to include tracking customers' activities without breaching their fundamental rights to privacy and reporting any criminal activity to the police once noticed. If such ISP turns a

---

43 Ibid.

44 Ibid.

45 An intranet is a private network accessible only to a company or an organisation's staff.

46 Moore, (n 16) 163.

47 Michel Van Eeten and others, 'The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data' [23 June 2010] <*http://www.pdfs.semanticscholar.org*> accessed 1 November 2017.

48 Ibid.

mail services for a fee.[35] Today, people connect the internet through a cable internet connection, provided by a local cable television company, or through a digital subscriber line (DSL), provided by a telephone company. When a customer dials into the system,[36] or connects to the system,[37] then the ISP provides the customer access to the internet and the web.[38] In order to confirm that customers do not exceed a monthly usage maximum, and to maintain records for billing purposes, each customer is assigned a temporary internet address, the Internet Protocol (IP). The IP address allows the ISP to locate customers when they are online.[39] Each customer is assigned a unique IP when they access the internet, thus providing each person an identifiable tag.[40] In certain cases, there are limited numbers of IP addresses available for use, and each address must be registered by the owner. Therefore, an ISP may have hundreds of thousands of IP addresses but have millions of customers. When a customer connects to his or her ISP, he or she is assigned an IP address that may or may not be one he or she has used in the past.[41] The process of constantly reassigning IP addresses upon each connection by the customer is known as dynamic IP addressing.[42] However, each time the IP address is assigned to a customer, the ISP's computers monitor which customer has been accorded the IP address, how long he or she maintains the address and from where he or she accessed the ISP's service. It should be noted that not all IP addresses are dynamic in

---

35 Moore, (n 16) 161.

36 Example, narrowband connections like a 56.6 modem.

37 Broadband connections such as cable internet or DSL

38 Moore, (n 16) 161.

39 Ibid.

40 An IP address normally appears in the following format and referred to as IPv6. The IPv6 format would be xxx:xxxx: xxxx:xxxx: xxxx: xxxx:xxxx:xxxx:xxxx with each "x" representing a hexadecimal value.

41 Moore, (n 16) 162.

42 Ibid.

speed leased lines so that they are less dependent on the telecommunication providers and can provide better service to the customers. An ISP is also sometimes referred to as an IAP (Internet Access Provider). ISP is sometimes used as an abbreviation for Independent Service Provider to distinguish a service provider that is an independent, separate company from a telephone company.[29]

ISP refers to a company that provides internet services, including personal and business access to the internet,[30] usually, for a monthly fee. The service provider provides a software package, username, password and access phone number. Equipped with a modem, one can log on to the internet and browse the World Wide Web (WWW) and USENE and send and receive e-mails.[31] ISPs also serve large companies, providing a direct connection from the company's networks to the internet. ISPs themselves are connected to one another through Network Access Points (NAPs).[32] Network Access Point is a point at which sections of the internet high-speed backbone are connected. ISPs are connected at Network Access Point so they can exchange packets.[33] The backbone of the internet actually consists of sections of high-speed fiber-optic cabling that are owned by different carriers. NAPs are places at which these carriers interconnect their lines so that the internet can function as a single entity.[34]

When people connect to the internet, they are not connecting directly into the internet or the web. Instead, the direct connection is made with their ISP. The ISP provides internet and e-

---

29 Ibid.

30 Vangie Beal, 'ISP- Internet Service Provider' <*http://www. webopedia. org>Term>ISP>* accessed 20 October 2017.

31 Ibid.

32 Ibid.

33 'Network Access Point (NAP) in the Network Encyclopaedia' <*http://www.thenetworkencyclopedia.com*>accessed 24 October 2017.

34 Ibid.

The nature of cybercrime includes the anonymity identity. The internet provides anonymity and safety. Unlike other forms of crimes wherein the person undertakes considerable risks, cybercrime provides the criminal with a cover because of the nature of the crime.[24] The cybercriminal leaves no physical foot-prints, finger-prints or other tangible traces, making it extremely difficult to track offenders down. Cybercrime being technologically driven, evolves continuously and ingeniously making it difficult for investigators to cope up with changes.

The diversity of cybercrime is an important aspect of its nature. Case studies provide an insight into the vast scale, reach and diversity of cybercrime.[25] From online bullying to human trafficking, the use of the cyberspace to plan, conduct and commit crime spans the traditional, physical, legal and structural boundaries of policing.[26]The variety of ways, techniques and reach of cybercrime is worthy of concern. For the totality of cybercrime to be tackled effectively, it requires the joint efforts of ISPs and the law. The question at this juncture is, what are the duties of ISPs.

3. Duties of Internet Service Providers (ISPs)

An Internet Service Provider (ISP) has been defined as 'a company that provides individuals and other companies access to the internet and other related services such as web site building and virtual hosting'.[27] An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the internet for the geographic area served.[28] The larger ISPs have their own high-

---

[24] 'Legal Point: Nature and Scope of Cyber Crime' *<http://www.legalpoint-india.blogspot.com>*accessed 22 October 2017.

[25] Staniforth, (n 21) 29.

[26] Ibid.

[27] Margaret Rouse, 'ISP (Internet Service Provider)' *<http://www.searchwindevelopment.techtarget.com> accessed* 24 October 2017.

[28] Ibid.

The nature of cybercrime includes the anonymity identity. The internet provides anonymity and safety. Unlike other forms of crimes wherein the person undertakes considerable risks, cybercrime provides the criminal with a cover because of the nature of the crime.[24] The cybercriminal leaves no physical foot-prints, finger-prints or other tangible traces, making it extremely difficult to track offenders down. Cybercrime being technologically driven, evolves continuously and ingeniously making it difficult for investigators to cope up with changes.

The diversity of cybercrime is an important aspect of its nature. Case studies provide an insight into the vast scale, reach and diversity of cybercrime.[25] From online bullying to human trafficking, the use of the cyberspace to plan, conduct and commit crime spans the traditional, physical, legal and structural boundaries of policing.[26]The variety of ways, techniques and reach of cybercrime is worthy of concern. For the totality of cybercrime to be tackled effectively, it requires the joint efforts of ISPs and the law. The question at this juncture is, what are the duties of ISPs.

3. Duties of Internet Service Providers (ISPs)

An Internet Service Provider (ISP) has been defined as 'a company that provides individuals and other companies access to the internet and other related services such as web site building and virtual hosting'.[27] An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the internet for the geographic area served.[28] The larger ISPs have their own high-

---

[24] 'Legal Point: Nature and Scope of Cyber Crime' *<http://www.legalpoint-india.blogspot.com>*accessed 22 October 2017.

[25] Staniforth, (n 21) 29.

[26] Ibid.

[27] Margaret Rouse, 'ISP (Internet Service Provider)' *<http://www.searchwindevelopment.techtarget.com> accessed* 24 October 2017.

[28] Ibid.

Convention, which identified several activities present in offences of cybercrime.[21] These activities served to shape what elements constituted contemporary cybercrime and included:

i. Intentional access without right to the whole or part of any computer system,
ii. Intentional interception, without right, of non-public transmissions of computer data,
iii. Intentional damage, deletions, deterioration, alteration or suppression of computer data without right,
iv. Intentional and serious hindering of the function of a computer system by inputting, transmitting, damaging, deleting, deterioration, altering or suppressing computer data,
v. Production, sale, procurement for use, importation or distribution of devices designed to commit any of the above crimes, or of passwords or similar data used to access computer systems, with the intent of committing any of the above crimes.[22]

These are pointers to the fact that cybercrime can take different forms. It shows the wideness of its scope. The intentional damage, deletion or suppression of computer data without permission or right amounts to cybercrime. This paper submits that there are actions certain people indulge in without the slightest idea that it is a crime. Cybercrime is highly complex, self-reinforcing, technologically advanced, geographically widespread and indiscriminate.[23]

---

21 Andrew Staniforth, *Blackstones's Handbook of Cyber Crime Investigation*, Babak Akhgar (ed) Francesca Bosco (ed) (1st edn, London: Oxford University Press 2017) 10.

22 Ibid.

23 'Nature, Prevalence and Economic Impact of Cyber Crime' <*https://www.aph.gov.au.*>accessed 20 October 2017.

committing the criminal act, but he or she has stored evidence on the machine.[17]

Casey's definition of computer crimes encapsulates when the computer is used as an instrument to perpetrate crime, when it is the focus of the crime and when it is used as a storage device. This definition describes the nature of cybercrime and the different ways the computer can be used to commit a crime.

Cybercrime has also been defined as any crime that involves a computer and a network, where a computer may or may not have played an instrumental part in the commission of the crime.[18] From this definition, it is clear that the term cybercrime actually refers to computer-related crime; however, some scholars consider computer crime as a subdivision of cybercrime that warrants its own definition and understanding.[19] Computer crime refers to a criminal activity in which a computer or an electronic information system is the vehicle, object or environment of the crime.[20] This paper submits that there are a number of terms employed to refer to this crime classification, including computer crime, cybercrime, hi-tech crime, digital crime, electronic crime, e-crime etcetera. These terms, which are capable of being employed in slightly different ways, all refer to the same class of criminal activities and it is almost a matter of choice which term is used.

There is no universally accepted definition of cybercrime. Acknowledging the global reach of cybercrime and the requirement to establish a common understanding of the threat and risks posed to multiple countries, the Council of Europe (CoE) adopted its Convention on Cybercrime Treaty, known as the Budapest

---

17 Ibid.

18 Ibid.

19 Ibid.

20 'Computer Crime, E-Crime, Cybercrime- Criminal Classification' <*http://www.lectlaw.com*>accessed 22 October 2017.

There needs to be an effective synergy and cooperation amongst these institutions to achieve a safer cyberspace.

This paper is divided into four parts. Part one focuses on the introduction. Part two discusses the nature and scope of cybercrime. Part three analyses the duties of ISPs in Nigeria. It also analysed the adequacy of these duties in enhancing cybersecurity. Part four examines international instruments like the Budapest Convention on Cybercrime and the E-Commerce Directive. It juxtaposes it with the law in Nigeria and draws lessons that can be learnt for Nigeria. Part five provides concluding remarks.

2. The Nature and Scope of Cybercrime

Traditionally, the term computer crime has been used to refer to criminal activities involving a computer that are made illegal through statute.[16] According to Eoghan Casey, a computer crime is a crime that involves a computer in one of the following ways:

i. The computer as an instrument of the crime. Here, the computer is used as a means of engaging in the criminal activity. Under this category, the crime cannot be committed without the computer being turned on and used in the commission of the act.

ii. The computer as the focus of a crime. Here, the computer is the intended target of criminal activity and is not necessarily used in the commission of the act.

iii. The computer as a repository of evidence. Here, the individual involved in a criminal act has not stolen the computer and has not used the computer as a means of

---

1999, National Information Technology Development Agency Act 2007, Nigerian Cybersecurity and Data Protection Agency.

16 Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime*, Shirley Decker-Lucke and Ellen Boyne (eds) (2nd edn, New York: Anderson Publishing 2011) 4.

policy work should be conducted to examine how ISPs could be called to the chain of security responsibilities of the internet.[13]

The scope and impact of cybercrime is global, it is propagating and diversifying expeditiously. The criminal justice response globally has increased tremendously; there are various international, national, cybersecurity and organised crime strategies cropping up daily in the fight against cybercrime.[14] This article argues that ISPs has a huge role to play in enhancing cyber security and curbing cybercrime. They are like guardians who should provide surveillance over internet consumers for the purpose of preventing crime or providing prompt response in the event that a crime is committed. There should be a legislative framework demanding this guardianship duty from ISPs in Nigeria to help police the cyberspace. ISPs can increase the lifetime value of her customers by providing security protection.

The central hypothesis outlined here is that ISPs should move from the checkbox mentality and embrace the cyber security craze. The era of compliance is over, it has been overtaken by security consciousness. They should take the necessary measures to enhance cyber security. This article identified gaps in the Cybercrime Act, 2015, regarding the duties and liability of ISPs in Nigeria. The existence, division and diversity of various autonomous institutions on cyber security in Nigeria draws back the fight against cybercrime. There exists a conflict in the area of power to detect, investigate and prosecute cybercrime in Nigeria amongst parallel government institutions and legislative Acts.[15]

---

13 The author engages in critical literature by relying on primary sources (articles on duties of ISPs) but it did not proffer solutions to the gap identified.

14 Interpol, International Telecommunications Union, The Police Commissioners' Conference Electronic Crime Working Party etcetera.

15 Nigerian Communications Act 2003, The Economic and Financial Crime Commission (Establishment) Act 2004, Advance Fee Fraud and other Fraud Related Offences Act 2006, Constitution of the Federal Republic of Nigeria,

broader knowledge of cyber threats that affects internet users and businesses, hence the need for ISPs to shoulder more responsibilities of the internet. The paper stated that according to Jennie Ness, a Regional IP Attache at U.S Commercial Service, the functions of ISPs include:

1. Transitory communications (serving as an information carrier): ISP acts as a mere data conduit, transmitting digital information from one point on a network to another at a user's request;
2. System caching: Retaining copies, for a limited time, of material that has been made available online by a person other than the ISP. Caching is technologically necessary to ensure internet speed and efficiency, particularly in terms of providing rapid access to popular content without overloading servers;
3. Storage of information on systems or networks at direction of users (hosting): Allowing users to post materials and host website for uses; and
4. Information location tools (searching): ISP provides internet search engines, Hyperlinks and Internet Directories.[11]

The paper finds that there is no specific law putting ISPs liable for end users' security. Although there are existing laws related to copyright, defamation, privacy, and similar crimes.[12] However, the laws did not put the ISPs liable for the users' illegal activities or end users' internet security instead it provided more immunity for ISPs. The paper concluded by suggesting that more research and

---

11 Ibid.

12 Examples of these laws in the United States are the Communications Decency Act, 1996 (CDA) and the Digital Millennium Copyright Act, 1998 (DMCA). The Electronic Commerce Directive (E-commerce Directive) in Europe was adopted in 2000.

economic growth. With these technological improvements come the increase in internet/computer crimes called cybercrime. There has been a lot of scholarly writings on the subject of cybercrime and the need to improve cyber security.[5] In fact, articles on cybercrime graze the front page covers of reputable journals around the world but the issue of ISPs duties in Nigeria to help curb cybercrime has been afforded very little attention. In the foreign scene however, legal commentators have written on the duties of ISPs and the need to expand this role to help curb cybercrime. Melissa Hathaway,[6] stated that the internet is a critical infrastructure in itself and a key component to other forms of critical infrastructure, underpinning economic and social activity at the global level. ISPs come in many forms and sizes and go by many names: the phone company, the cable company, the wireless company etcetera.[7] The paper added that ISPs are the internet stewards that plan and manage resources, providing reliable connectivity, and ensuring delivery for traffic and services. It should shoulder more responsibilities for the stewardship of the internet.[8] It concluded that ISPs have an unparalleled access into and view global networks, which gives the proper tools to detect cyber intrusions and attacks as they are forming and transiting towards their targets.[9] Hassan Shuaibu,[10] stated that ISPs have

---

5 Peter Grabosky, *keynotes in Criminology and Criminal Justice Series Cybercrime*, (New York: Oxford University Press 2016).

6 Melissa E. Hathaway, 'Stewardship of Cyberspace: Duties for Internet Service Providers' [March 2012] <*http://www.belfercenter.org*> accessed 24 October 2017.

7 Ibid.

8 Ibid.

9 Ibid. This paper embodies rich and substantive context but it was tailored for developed countries and does not address the gaps identified in Nigerian law.

10 Hassan Shuaibu, 'A Review of Responsibilities of Internet Service Providers Towards their Customers' Network Security' [March 2013]<*http://www.academia.edu*>accessed 30 October 2017.

duties and measures ISPs should conform to and help secure the internet ecosystem.

1. Introduction

According to Jeh Johnson, the former Secretary of the United States Homeland Security:

> Cybersecurity is a shared responsibility, and it boils down to this: in cybersecurity, the more systems we secure, the more secure we all are. We are all connected online and a vulnerability in one place can cause a problem in many other places. So everyone needs to work on this: government officials and business leaders, security professionals and utility owners and operators.[1]

In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the internet.[2] Over 60 percent of all internet users are in developing countries, with 45 percent of all internet users below the age of 25 years.[3] By the year 2020, it is estimated that the number of networked devices will outnumber people by six to one, transforming current conceptions of the internet.[4]

The increase in the availability and accessibility of the internet has positively improved societal communications and

---

* Ifeoma E. Nwafor, LL, B Hons (UNIZIK), LLM (NIG), BL, FCArb (Nigerian Institute of Chartered Arbitrators), Doctoral Candidate, University of Nigeria, Enugu campus. Lecturer, Faculty of Law, Godfrey Okoye University. Email: ifeomanwafor900@gmail.com.

1 'Remarks by Secretary of Homeland Security Jeh Johnson at The White House Cybersecurity Framework Event' [12 February 2014] <*http://www.dhs.gov>news>2014/02/12*>accessed 13 October 2017.

2 'Comprehensive Study on Cybercrime- United Nations Office on Drugs and Crime' [February 2013] <*http://www.onodc.org>organisedcrime*>accessed 1 October 2017.

3 Ibid.

4 Ibid.

Chapter Three

CYBERCRIME IN NIGERIA: THE ROLE OF INTERNET SERVICE PROVIDERS IN ENHANCING CYBERSECURITY

By

Ifeoma E. Nwafor *

Abstract

Internet connectivity has shortened time and space. It has enhanced the transfer of information and provided unlimited opportunities for commercial, educational, communication, social and individual activities. These electronic and globalized benefit is accompanied with an increase in cybercrime activities. Nigeria is ranked highly in global internet crimes and in consequence, economic growth has plummeted, and international investors' confidence is rock bottom. Data breaches fundamentally, affects consumers' confidence in the cyberspace. Internet Service Providers (ISPs) have a crucial role to enhance cyber security and boost internet users' trust in the internet ecosystem. This article examined the ISPs role in promoting cyber security. It found that ISPs are not doing enough to police or secure the cyberspace. The objective of this paper is to offer insights on the copious opportunities ISPs can furnish to cyber security enhancement based on the edge and bearing they possess in the cyberspace. ISPs can offer more than the compliance-checkbox; it should provide continuous protection for consumers. This article adopts the doctrinal method of legal research. It analyses the Cybercrime Act 2015. It found that there are gaps with respect to the duties of ISPs and in the area of enforcement. It canvasses for an amendment of the Act to specifically provide the strategic

GODFREY OKOYE UNIVERSITY

LAW JOURNAL

Journal of Contemporary Legal and Allied Issues

Volume 1 No. 1 2018

CONTENTS

Published by the Faculty of Law, Godfrey Okoye University, Enugu, Nigeria.