THE QUAGMIRES OF THE AMOEBIC INTERNET: LAW AND TECHNOLOGY TO THE RESCUE*

Abstract

The word, quagmires in the topic of this paper opens up the floor as to the dangerous situation into which the emergence of this phenomenon called, the Internet, has launched the society. Ever since the Internet came into operation, the entire world has been reduced to the same close proximity, and online freedom of expression has become virtually unlimited. On the Internet, anyone anywhere can express himself or herself, no matter how singular, without fear of being coerced into silence or compromise. The Internet is open, global, user-controlled, decentralized, inexpensive, abundant, and makes use of independent infrastructure. The Internet is amoebic because it is not stereotyped, as a result of which it can easily be manipulated. All these features, among others, have combined to convey the quagmires brought about by the Internet technology. Adopting the doctrinal method of research, this paper therefore discusses the various circumstances or situations evidencing the quagmires of the amoebic Internet. It equally identified the roles of law and technology in arresting these quagmires, pointing out that there must be a globally galvanized effort in order to achieve success. The paper concludes that since the Internet itself is a technological phenomenon, the best way to handle the quagmires is through a technological approach backed by law.

Keywords: *The Amoebic Internet, Quagmires, Law, Technology, Rescue.*

1. Introduction

This paper talks about the quagmires of the amoebic Internet and brings out the role of law and technology in curbing the menace. The word, quagmires depicts a difficult or dangerous situation. This means that the emergence of the Internet technology has brought about some inimical challenges very difficult to handle. The quagmires being referred to here may be of two dimensions. The first dimension is about the problems emanating from the use of the Internet such as the use of the Internet to commit fraud and other crimes generally known as cybercrimes. The second dimension is about the problems frustrating the efforts geared towards controlling the activities on the Internet in order to prevent the occurrence of criminal, harmful and illegal activities on the Internet. Although, these quagmires may be considered as constituting a single whole, the distinction between them is very lean. One important point of the distinction between them is that one dimension leads to and reinforces the other. Hence, the second dimension can be said to be the reinforcement factor of the first dimension. These quagmires are difficult to handle because of the amoebic nature of the Internet. The Internet is said to be amoebic because it lacks a fixed form and supporting structures, as a result of which even the United States of America that invented the technology does not have a very clear solution for its definite regulation. Be that as it may, it is the position of this paper that both law and technology have a significant role to play in addressing the quagmires of the amoebic Internet so far. It is important to bear in mind that this paper is particularly concerned with the second dimension of the quagmires. This discussion will herein continue with meaning of the Internet.

2. The Internet

The Internet has not really confined itself to a particular definition. At best, this technology called the Internet can only be described.[1] Accordingly, it can be described as an electronic network which may be wired or wireless by which one can store, transmit data to or receive data from any distance across the world with the use of a computer system within the shortest possible time. The Internet is the large system of connected computers around the world which allows people to share information and communicate with each other using electronic facilities, with or without inconsequential barriers of time and distance.

*** Kenneth Uzor EZE (LLB, BL, LLM, PhD, PGDIT, MIAD, GMNIM, pnm),** Head of Academy Advancement Unit and Head of Department of Public and Private Law, Nigeria Police Academy, Wudil - Kano, Nigeria. E-Mail Address: skennue@yahoo.com. Phone No.: 08068686518.

[1]K U Eze, A Peep into Regulation of the Internet Use towards Ensuring Internal Security: The Role of the Nigeria Police Force, a paper presented at the National Conference on Police, Internal Security and Governance in a Democratic Nigeria, May 27 – 30, 2018, Nigeria Police Academy, Wudil, Kano State, Nigeria.

It is a system whereby networks are interconnected in a manner which permits each computer on any of the networks to communicate with computers on any other networks in the system.[3] The Internet in simple terms is a network of the interlinked computers networking worldwide, which is accessible to the general public. These interconnected computers work by transmitting data through a special kind of packet switching which is known as the Internet Protocol.[4] These networks enable the Internet to be used for various important functions which include the several means of communications like the file transfer, the online chat and even the sharing of documents from web sites on the world wide web. The use of the Internet Protocol in the Internet is the integral part of the network, as they provide the services of the Internet, by different layers organization through the Internet Protocol data packets. There are other protocols that are the sub-classes of the Internet Protocol itself, like the Transmission Control Protocol (TCP), and the Hypertext Transfer Protocol (HTTP) . While the Internet is said to have its origin from United States of America, no one actually owns the Internet, and no single person or organization controls the Internet in its entirety. The Internet is more of a concept than an actual tangible entity, and it relies on a physical infrastructure that connects networks to other networks.

The basic function performed by the Internet is extremely simple. It transports digital information from one computer to another, and nothing more.[5] This means that at the functional level, the Internet is not more than a communication technology. The meaning of the information communicated through the Internet is completely irrelevant to its transport; that meaning is determined by the software which receives the information. Any type of information which can be translated to digital form can be transported. The most common types of information are texts, numerical data, images, sounds and video. Any additional functions which are effected through the Internet are not performed by the Internet itself, they are services which are provided by one or more of the players involved and all these services are performed by the exchange of digital information. The transport function is performed by copying the digital information from one computer to another until a copy reaches the receiving computer. The information, however, is not sent in a continuous stream, instead, the sending computer splits the information into discrete packets or datagrams, each addressed to the receiving computer, which reassembles the information ones the packets have arrived.[6] The intermediate computers work simply on the addresses of each packet, forwarding it to another computer until it reaches its destination. It is not compulsory that these packets must follow the same route, or arrive at the same time, or in any particular order.[7]

From the foregoing, it is clear that there will be more persons involved in any transmission of information than simply the sender and receiver. The packets containing the information transmitted will have been copied by one or more intermediate computers which may not be the same computers for each packet. For the purposes of legal analyses, it is simplest to divide the actors in any Internet information exchange into two, namely:

1. The parties to the Internet information exchange, including the computers of sender and recipient which are at the end of the exchange. The Internet technical language for this group of actors responsible for sending and receiving is called 'hosts'. This should not, however, be confused with the hosting of a website, whereby one organisation provides the space to store the files which make up another's website and provide access to it. A host computer or simply 'host' is the ultimate consumer of communication services. A host generally executes application programmes on behalf of users, employing network and/or the Internet communication services in support of this function.
2. Intermediate computers, including the other computers which receive and pass on packets. This group of actors are known as 'routers' or 'gateways'. These 'routers' or 'gateways' are packet-switching computers by which the networks are interconnected.

[3] D. Ashaolu, & A. Oduwole, *Policing Cyberspace in Nigeria, a publication in honour of Col. Sani Bello (Rtd)* (Nigeria: Life Gate Publishing Co. Ltd, Ibadan, 2009) p. 3.
[4] A protocol is an algorithm for recognising and dealing with a piece of information.
[5] Reed, C, Internet Law Text and Materials (2nd edn, India: Universal Law Publishing Co., New Delhi, 2010) p. 8.
[6] *Ibid.*
[7] K U Eze, 'A Review of the Problems in Regulating the Internet Use: Enforcement Mechanisms against Cybercrimes under International Law', A PhD Research Dissertation presented to the Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria, June 2016, p. 40.

The above shows that the Internet is not an entity but a communication infrastructure or technology, to the extent of being a thing, it is a network of networks, all internetworking with each other by passing data packets.[8] Users communicate with each other across the Internet using client/server technology. Here, one information exchange or communicating party runs client software that does the function of requesting information, while the other information exchange party runs server software that handles and executes the request. A good example of this scenario is viewing a web page where the user enters the address called the Uniform Resource Locator[9] of the page into his browser software.[10] This is the client software which causes a request to be produced for the page and the request is sent through the Internet to the computer on which the page is stored. The web server software running on that computer responds to the request by sending the packets which make up the page to the browser software. The browser then reassembles them and displays the page.[11] A user's client software and the other party's server software are able to exchange packets of information across the Internet because all the computers involved use common protocols to define how a packet should be dealt with.

3. Quagmires of the Amoebic Internet

We shall herein discuss those challenges which have rendered the Internet technology a quagmire. It has already been noted that this paper is particularly concerned with the second dimension of the quagmires as reflected in the introduction of this paper. Without fear of repetition, the second dimension is about the problems frustrating the efforts geared towards controlling the activities on the Internet to ensure that neither criminal or harmful activities are carried out on the Internet nor illegal or wrongful contents freely created, distributed and accessed on the Internet by the netizens.[12] These challenges bring out the difficulties, problems and frustrations always experienced in trying to bring the freedom in use of the Internet under control. They are hereunder discussed seriatim.

Heterodox Nature of the Internet

Something is heterodox if it is different and in opposition to generally accepted beliefs or standards.[13] The Internet is heterodox because it does not conform to the orthodox means and standards of other communications technology. The Internet is one technology that defies the normal regulation applicable to other information communication technology. Generally, the Internet tends to be like a flowing water that no one can control its movement. Any attempt to block the movement of the water will certainly create two possible chances, that is, as the flowing water becomes fuller: first, there is the possibility that the water would start flowing over the blockage or, second, there is another possibility that the water may find its way through another route altogether, by the corners of the blockage. Similarly, any attempt to regulate the Internet may be futile since the length and capacity of the technology is yet to be comprehensively fathomed. Indeed, the Internet is such that if you await it in one direction, it will burst out in another direction. This explains why the numerous laws aimed at checking its operations simply come to naught. The Internet is the most independent and pluralistic of all media. There appear to be no end to the scientific and technological breakthrough in the area of the Internet. The Internet technology is not stereotyped. In short, the Internet is scientifically and technically amoebic in nature. And because it is amoebic, it can be easily manipulated. Even cyber criminals, most of whom, have neither academic nor technical knowledge of computer now experiment with the computer in the name of making use of the Internet. And in the course of their experiment, they discover new areas unknown to the so called Internet experts. This is why governments and other institutions or organisations have continually experienced security threats or real attacks on their Internet

[8] D Lars, 'The Internet and the Elephant', *International Business Lawyer* (1996) p. 151. Cited in Reed, C, Internet Law Text and Materials (2nd edn, India: Universal Law Publishing Co., New Delhi, 2010) p. 10.

[9] The Uniform Resource Locator is made up of the domain name, directory structure, filename. Example is <www.polac.edu/law/index.html>.

[10] This browser software may be Mozila Firefox or Internet Explorer or Netscape Navigator, etc.

[11] C Reed, *Internet Law Text and Materials* (2nd edn, India: Universal Law Publishing Co., New Delhi, 2010) p. 10.

[12] Netizens simply means the Internet users.

[13] Cambridge University, *Cambridge Advanced Leaner's Dictionary* (3rd edn, Cambridge: Cambridge University Press, 2010) p. 676.

settings without being able to dictate and understand all the details.[14] As more and more criminals are aware of potentially large economic gains that can be achieved with cybercrimes, they tend to switch from simple adventure and vandalism to more targeted attacks, especially platforms where valuable information highly concentrates. In a jiffy, the nature of the Internet forbids the regulation of the Internet use. This therefore constitutes a serious problem because, in the first place, most individuals, institutions and governments do not want to talk about the regulation of the Internet use based on the thinking that the Internet defies regulation by its heterodox nature. What is more, this heterodox nature of the Internet has created a level of fear in the people that is almost reaching a despondent level. It is, however, hoped that the effective utilization of law and technology would certainly bring such quagmires to book.

Problem of Trans-Border Data Flows

Developments in global communication networks and business processes have increased the volume of trans-border data flows which have adequately been enhanced by the Internet facility. Data transfers in areas like human resources, financial services, education, e-commerce and health research, etc. are now integral parts of the global economy. Advances in technology mean that data can be transferred quickly and stored indefinitely. Data transfers enable a globally distributed approach to tasks which takes advantage of expertise in multiple locations around the world and around the clock. In addition to bringing business efficiencies and convenience for users, however, changes to global data flows have also elevated the risks to privacy. Wrong-doers seek to exploit technology to expose data,[15] mostly for financial gain. In particular, this brings to focus in this paper the problems relating to data security breaches in cases with a cross-border dimension. As with spam and cross-border fraud, protecting privacy in a global environment depends on cross-border co-operation. However, given that organisations do not usually find it advantageous to publicize their security breaches, the scale of the problem may not be well ascertained. A number of privacy breach cases have impacts beyond the borders of the country in which the breaches are reported,[16] the cross-border dimensions are not often noted by the authorities or in the press. Also, whether privacy complaints will follow the domestic complaint trends is not very clear. First of all, individuals may not be aware of the use of their personal data beyond national borders. Sometimes, they may not even realise that their complaint would involve a foreign institution. They may not know to whom to complain with a cross-border problem. Indeed, even in a purely domestic context, individuals may not know to whom they should complain.[17]

Freedom of Expression Versus Harmful Content on the Internet

Another problem is the compelling issue of protection of free use and restriction of harmful content on the Internet. There is a massive amount of pornography of all kinds on the Internet. Many children on-line have come across web sites that upset or embarrass them. Also, there are some sites which propagate extremist views, often of a terrorist, racist or political nature. While almost all of these may be legal and a free society should permit access to such materials, many Internet users, especially parents, teachers and those with responsibility for children will want to place some limitations on access to such materials. It has been argued that any system of controls on the content of the Internet represents a breach of the individual's right to freedom of expression and press and that such a right is absolute and cannot be qualified without irreparable damage to civil liberty in a free society. But all rights have

[14] In various governments and other institutions today, the incidence of cybercrimes committed through the Internet has become very rampant but most institutions and organisations feel so shy to expose same for the sake of preserving their values.

[15] In Japan, the Cabinet Office reported that the number of personal information breach cases publicly announced by organisations in 2005 exceeded 1500.

[16] In 2005, media reports indicated that the identities of customers could be easily bought from call centres operated for United Kingdom banks in India. June 2006 brought reports of cross-border data breaches in the United Kingdom involving the data of 2500 United States employees. In the same month, police in India arrested an employee of the customer service centre of a multinational financial institution for illegally accessing customer account information from the United Kingdom customers that resulted in the theft of GBP 200, 000. In July 2006, a computer hacker in Germany gained access to the computer system of a local government agency in the United States that contained personal information on 4, 800 public housing residents.

[17] A study in Norway found that only 33% of Norwegians know that the Data Inspectorate is the authority responsible for the protection of personal data. Available at <http://www.toi.no/article17922> accessed on August 14, 2018.

to be qualified because absolute rights threaten other rights. An unrestricted right to freedom of expression and press would threaten the right of children to be free from abuse or molestation and the right of ethnic and political minorities to live their lives free from racial and political intimation and violence.

Problem of Jurisdiction

One major feature of the Internet that has continued to pose a problem to its users is the absence of a defined territory or boundaries. By its very nature, the Internet is a network of computers with different technologies. In the real world, geographical or natural boundaries serve to define rights and duties. However, for the Internet, there are no territorial or geographic boundaries. Thus, once a material is on the Internet, it can be accessed from anywhere in the world. The rise of this electronic medium that disregards geographical boundaries throws the law into disarray by creating an entirely new phenomenon that needs to become the subject of clear legal rules that cannot be governed satisfactorily by any current territorially-based law.[18] Any insistence on reducing online transactions to a legal analysis based on geographic terms presents, in effect, a new problem on a global scale. Hence, which national law applies when a person in Nigeria orders for goods offered online by another person in United Kingdom and pays for it with credit based on a credit card information phished[19] from a victim in South Africa? Where can a person injured by any defect in this process sue or out of these three jurisdictions, which one has the authority to prosecute the cybercriminal who phished someone's credit card information in the above scenario? Which country will enforce the judgment obtained in this case? These, among others, are the very plausible jurisdictional questions that have emerged in the Internet technology. Basically, the public interact on the Internet in two primary ways: either putting information on the Internet or taking information out of the Internet. In the eyes of the law, then, there are two distinct actors on the Internet: the sender and the receiver. It should be noted here that these sender and receiver might be one sender to one receiver or one sender to many receivers. Under this phenomenon, the sender and the receiver act like spies in the classic information drop such that the sender puts information on a location on the Internet, and the receiver accesses the said information at a later time. And neither of these actors need be aware of the other's identity.

However, unlike the classic information drop, there need not be any specific intent by these actors to communicate in the first place. By this very phenomenon, information on the Internet are accessed by hundreds of thousands of people from all over the world. In both civil and criminal law, most actions taken by senders and receivers present no jurisdictional difficulties. In this regard, a country can forbid, on its own territory, the uploading and downloading of the Internet materials it considers harmful to its citizens or interests. Thus, a country may decide to forbid anyone from uploading a pornographic site from its territory, and can forbid anyone within its territory from downloading or accessing the said pornographic site on the Internet. For example, the United States Supreme Court declared the Communications Decency Act of 1996 unconstitutional for over-breadth and vagueness on a facial challenge,[20] but therefore did not have a chance to address its international implications. Apart from the internal limitations of the United States Constitution, there is little doubt that, under international law, the United States has the jurisdiction to prescribe law regulating the content of what is uploaded from United States territory but accessed in another jurisdiction through the Internet or what is uploaded in another jurisdiction but accessed in the United States through the Internet. Had the Supreme Court of United States been presented with an actual case or controversy concerning the application of the Communications Decency Act of 1996 to a foreign national resident abroad, the Supreme Court would have had to consider the extraterritorial application of the law as written, and could have been expected to apply the presumption against extraterritoriality and to have circumscribed the Communications Decency Act of 1996 in that regard. The early American case of *The Schooner Exchange v*

[18] See B. Oladipo, *Information Technology and the Law: the Nigerian Perspective* (Nigeria: Legal Digest Publishing, 2002) pp. 95 - 96.

[19] Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. It is the fraudulent acquisition, through deception, of sensitive personal information such as passwords and credit card details by masquerading as someone trustworthy with a real need for such information. It is a form of social engineering attack against a person after obtaining the person's private information, particularly relating to the persons electronic contacts.

[20] See the case of *Reno v ACLU*, 117 S. Ct. 2329, 2346-48 (1997).

McFaddon[21] demonstrates how this problem could manifest. This case held that a French war vessel was not subject to American law, although it was in an American port. Applying this to the Internet, a website would be ascribed the nationality of its creator, and thus not be subjected to the law of wherever it happened to be accessed. Some states in the United States of America seek to exercise jurisdiction over actors on the Internet outside their own territorial boundaries. Minnesota is one of the first jurisdictions to attempt a general exercise of such jurisdiction. Minnesota's Attorney General, Hubert Humphrey III, issued a memorandum stating that, 'Persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws.'[22] A federal district court and the Minnesota Court of Appeals have applied the rationale of this memorandum and found personal jurisdiction based merely on the fact that information placed on the Internet was downloadable in the state in question. The opinion in *Minnesota v Granite Gate Resorts*[23] (a case argued for the state by the very same Hubert Humphrey III), accepted the Attorney General's argument and asserted jurisdiction over the website owner based in part on the fact that, "during a two-week period in February and March 1996, at least 248 Minnesota computers accessed and 'received transmissions from' appellant's websites. Of course, considering the nature of the Internet, all information on the Internet may be downloaded in Minnesota, and such an eventuality is always foreseeable. Therefore, Minnesota's rule makes all actors on the Internet subject to Minnesota law, the actor's location notwithstanding. It is submitted that if every state in the United States of America and elsewhere takes this approach, the result would be unbearable, especially for multinational corporations with attachable assets located all over the world. '[T]he resolution of these matters must be addressed at the national, if not international, level.'[24] Until fully addressed, jurisdictional questions relating to the Internet use will continue to be a quagmire.

Problem of Attribution over Crimes Committed on the Internet

Before jurisdiction over crime committed on the Internet even comes into play, it is necessary to discover where and who the criminal is, without which the tracking down and possible prosecution of the criminal would be rendered impossible. The complexity and anonymity of crimes committed on the Internet have made it difficult to attribute same to a specific individual, organization or state.[25] The major ingredient of free expression and the protection of privacy is the ability to express oneself without fear of retribution. This is very practicable on the Internet, where contents can be authored anonymously or pseudonymously. There are numerous services that will mask a user's Internet protocol address by routing traffic through various servers, usually for a fee.[26] This means that one can anonymously publish and disseminate prohibited materials such as pornographic materials online. Due to that feature, cybercriminals can openly carry out their operations without being caught especially when they can even use 'innocent machineries' as zombies in the operation. This makes the attribution of cybercrimes to the actual offenders very difficult. Under this circumstance, the tracking down of the cybercriminal may be rendered impossible. In the case of cyber-attacks generally, convincing evidence is hard to find given the anonymity of the technology involved, attribution of a cyber-attack to a specific state may be very difficult. While a victim state might ultimately succeed in tracing a cyber-attack to a specific server in another state, this can be an exceptionally time consuming process, and even then, it may be impossible to definitively identify the entity or individual directing the attack. For example, the 'attacker' might well have hijacked innocent systems and used those systems as 'zombies' in conducting attacks.[27] In 2007, Estonia experienced extensive computer hacking attacks that lasted several weeks. In 2008, during the brief Georgia-Russia War over South Ossetia, Georgia experienced cyber-

[21] The *Schooner Exchange v McFaddon*, 11 U. S. (7 Cranch) 116 (1812).

[22] Memorandum of Minnesota Attorney General (July 18, 1995), available at <http:llwww.state.mn. uslebranchlag> accessed on February 18, 2019.

[23] *Minnesota v Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (1997).

[24] Florida Attorney General, Formal Opinion: AGO 95-70 (Oct. 18, 1995).

[25] K U Eze, 'Defining the Term, Cyber Crime and Reviewing the Problems Militating against its Control under International Law', *Journal of Public and International Law*, Ahmadu Bello University, Zaria (2018) vol. 8, p. 158.

[26] S Deb, 'What Makes Laws So Difficult to Enforce' (January 26, 2011). Available at <www.tecrepublic.com> accessed on February 24, 2019.

[27] D E Graham, 'Cyber Threats and the Law of War' (2010) 4 *J Natl Security L & Policy*, 87, 92 (Citing Jensen E., 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stanford J Intl L*, 232 – 235 and R Lehtinen *et al*, *Computer Security Basics* (2nd ed, 2006) p. 81.

attacks similar to those suffered by Estonia in the previous year. Also, in 2009, computer malware, known as the Stuxnet worm, was released apparently by one or more governments to slow down the progress of Iran's nuclear programme. In all these cyber-attacks, there was no convincing evidence to attribute same to the respective attackers.[28] Hence, cybercriminals exploit the rights and privileges of this anonymous society, made possible by the amoebic Internet to illegally and outrageously benefit themselves at the expense of their victims. In 2009, Eugene Kaspersky identified the relative anonymity of the Internet users as a key issue that enables cybercrimes and proposed Internet 'passports' for individuals and accreditation for business to help combat the problem.[29]

In the United States of America, the attribution issue is further highlighted in the November 2014 revelation of a breach at Sony Pictures Entertainment (SPE) by actors known as the 'Guardians of Peace'. The Federal Bureau of Intelligence (FBI), in its investigation of the breach, noted that it

> consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and confidential communications. The attacks also rendered thousands of SPE's computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company's business operations.[30]

There has been debate among officials, scholars, reporters, and others about the true source of the breach. As of December 2014, the FBI leading an interagency effort had attributed the hack to North Korea. In its attribution, the FBI cited malware linked 'to other malware that the FBI knows North Korean actors previously developed', 'significant overlap between the infrastructure used in this attack and other malicious cyber activity the United States government has previously linked directly to North Korea', and tools similar to those used in a 2013 North Korean cyber-attack against South Korean banks and media outlets.[31] Nonetheless, experts critical of this attribution noted that the evidence linking North Korea to the SPE breach is not definitive.[32] Attribution continues to be a challenge in identifying both public security and national security threats. In the 2012 Worldwide Threat Assessment of the United States Intelligence Community, James Clapper, Director of National Intelligence noted the challenges in cyber actor attribution. More specifically, he noted that:

> two of our greatest strategic challenges regarding cyber threats are: (1) the difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, *definitively attributing them* (emphasis added), and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber-attacks; and (2) the highly complex vulnerabilities associated with the IT supply chain for US networks.[33]

The United States FBI, for one, has bolstered its efforts to better attribute cyber threats to specific sources and motives. Through the Next Generation Cyber Initiative, the FBI is developing agents to connect with critical infrastructure components and computer scientists to 'extract hackers' digital signatures' and determine their identities, all to help concretely attribute a specific malicious actor to a particular cyber incident. Similarly, relevant agencies and departments of various countries are making significant investments in forensics to address this

[28] However, the attack against Georgia was suspected to have been perpetrated by Russia while United States of America and Israel were suspected in that of Iran.
[29] S Deb, 'What Makes Cybercrime Laws So Difficult to Enforce', *loc. cit.*
[30] Federal Bureau of Investigation, 'Update on Sony Investigation', *press release*, December 19, 2014.
[31] *Ibid.*
[32] See, for example, G Andy, 'FBI Director: Sony's "Sloppy" North Korean Hackers Revealed Their IP Addresses', *Wired: Threat Level*, January 7, 2015; Pierluigi P., 'Sony Pictures Hack: Is North Korea Innocent or Guilty?', *InfoSec Institute*, January 11, 2015; and S Michael., 'Accurately Attributing the Sony Hack is More Important than Retaliating', *Georgetown Security Studies Review*, January 13, 2015. All cited in K Finklea & C A Theohary, 'Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement', January 15, 2015, available at <https://fas.org/sgp/crs/misc/R42547.pdf> accessed on February 15, 2019, p. 12.
[33] Office of the Director of National Intelligence, Unclassified Statement for the Record on the Worldwide Threat Assessment of the United States Intelligence Community for the Senate Select Committee on Intelligence, January 31, 2012, p. 8.

problem of attribution.[34] Attribution, however, may be more important for government for the purpose of law enforcement than for private sector organizations. Law enforcement agencies, through their investigations, may strive for attribution so that the actual perpetrator may be prosecuted. Industries and organizations, however, may be less concerned and may focus more on damage control and prevention regardless of the actor or his motivations.[35]

4. **Role of Law in Curbing the Quagmires of the Amoebic Internet**

Law as a lubricant to the engine room of the society is used to provide quick solutions to the societal problems. Some of those societal problems as already identified in this paper are said to have emanated from the emergence and use of the amoebic Internet. The role of law in curbing the quagmires of the amoebic Internet cannot be over-emphasized. There are actually two approaches by which the law may come in to the rescue of the society from these quagmires. These include: the constitutional approach and statutory approach. These approaches are discussed below.

Constitutional Approach

This approach makes the Constitution of the country the prime determinant of what is 'acceptable' on the Internet. In Nigeria, for instance, section 39 of the 1999 Constitution[36] provides for 'freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference'. The language of section 39 is broad enough to encompass all ideas and information directed to an individual or group of individuals, including electronic mail, chat, and other forms of person(s) to person(s) communications. Given that the Internet's root is in the exchange of information, section 39 of the 1999 Constitution seems particularly apt for the protection of communications on the Internet without interference. In accordance with section 39 of the 1999 Constitution, the ' freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference' seems particularly relevant to 'browsing' the Internet through search engines, portals and hyperlinks. In particular, the freedom to 'impart' information seems directly applicable to blogging and sharing information, through social network sites, and the freedom to 'receive' information encompasses the exchange of e-mail, the reading of web pages and the downloading of information. Section 37 equally provides for right to private and family life.[37] These freedoms are, however, limited under section 45 of the same Constitution 'in the interest of defence, public safety, public order, public morality or public health; or for the purpose of protecting the rights and freedoms of other persons.' In line with these limitations, the government may put in place policies or laws mandating the Internet users and the Internet Service Providers to disclose their identities for the contents they allow on the Internet. The government of Brazil abhors anonymity in its Constitution but guarantees freedom of expression in the same clause.[38] Some attacks on anonymity focus on users of cyber cafes or other public access points. Italian government, for example, requires the Internet cafes to identify and register users.[39] But in the case of *Reno v American Civil Liberty Union,*[40] the Supreme Court of United States of America, as part of constitutionally ensuring freedom of expression on the Internet, declared the Federal Communications Decency Act, 1996 unconstitutional as vague and overbroad. The said Act sought to protect children from harmful material by making it a crime to 'make available' online in a manner that anyone under eighteen years of age could access any 'indecent' or 'patently offensive' messages. Classically, this marked the United States of America's constitutional approach as efforts to enact relevant legislations for regulation of the Internet use have fallen foul of

---

[34] See for instance, United States Department of Defense, 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City', *news transcript*, October 11, 2012.

[35] Finklea & Theohary, 'Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement', *loc. cit.*

[36] Constitution of the Federal Republic of Nigeria, 1999 (as amended).

[37] Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) provides thus: 'The private citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'.

[38] Articles 4 and 5 of the Constitution of Brazil, 1988.

[39] M Sanminiatelli, 'Anti-Terror Law Forces Cybercafe Owners to Take Names' (2005), available at <http://www.usatoday/tech/news> accessed on July 13, 2018.

[40] *Reno v American Civil Liberties Union* (*Supra),* footnote 42 of chapter one, p. 19. The Supreme Court decision is available at <htt://www.law.cornell.edu/supct/html/96-511.ZS.html>, accessed on February 2, 2019.

the United States Constitution, in particular the first amendment on freedom of expression. The case explored the unique features of the Internet technology as they relate to the legitimacy of government controls using this constitutional approach

Statutory Approach

This approach makes a specific piece of legislation the prime determinant of what is 'acceptable' on the Internet. Classically this is the approach in Australia where the Broadcasting Services Amendment (Online Services) Act, 1999, regulates online content. This Act requires Australian Internet Service Providers to prohibit access to or remove from their web sites materials rated as illegal.[41] Under the guise of promoting civility or preventing crime, governments may force users to identify themselves online. Under the law of South Korea, popular websites are required to collect the names and national identification numbers of users before they can post comments or upload content.[42] Some governments also limit the use of encryption technologies. For example, Egyptian law forbids use of encryption technologies without permission from the telecommunications regulatory authority, the armed forces, or national security entities.[43] In Nigeria, under the Advance Fee Fraud and other Fraud Related Offences Act, 2006, 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 - full names; residential address, in the case of an individual; corporate address, in the case of corporate bodies.[44] Moreover, any person or entity who in normal course of business provides telecommunications or the Internet services or is the owner or the person in the management of any premises being used as a telephone or Internet cafe or by whatever name called shall be registered with the Economic and Financial Crime Commission and maintain a register of all fixed line customers which shall be liable to inspection.[45] Furthermore, section 7 (1) of Nigeria's Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, provides that: 'From the commencement of this Act, all operators of a cybercafé shall – (a) register as a business concern with Computer Professionals' Registration Council in addition to a business name registration with the Corporate Affairs Commission, and (b) maintain a register of users through a sign-in register and the register shall be available to law enforcement personnel whenever needed.' South Korea requires websites to obtain users' real names and national identity numbers before posting any comments or uploading any user-generated content.[46]

5. Role of Technology in Curbing the Quagmires of the Amoebic Internet

Technology has to do with application of practical knowledge, tools and methods for manufacturing, productive and development processes. Technical knowledge relates to the operation of a machine or system towards achieving a particular purpose. This means that considering the architectural composition of the Internet, it is itself a technology, that is, communication technology. As a communication technology, it has obviously introduced a world of liberal communication where individuals and groups can interact without barriers as to race, social class,

[41] The Act came into force in January 2000.

[42] M Aaron, 'South Korea Passes Cyber Defamation Law', Internet Defamation Blog (May 4, 2009), available at <http://internetdefamationblog.com/tag/cyber-defamation-law/> accessed on January 30, 2019.

[43] See Article 64, Egypt Telecommunication Regulation Law, Law No. 10 of 2003, available in English at <www.tra.gov.eg/uploads/law/law_en.pdf> accessed on January 30, 2019.

[44] See section 12 (1) of the Advance Fee Fraud and other Fraud Related Offences Act, 2006. A breach of this provision on the part of a subscriber attracts an imprisonment for three years or fine of N100, 000 upon conviction. And on the part of the person or entity providing the service, shall upon conviction be liable to a fine of N100, 000 and forfeiture of the equipment or facility used in providing the service.

[45] *Ibid*, section 13 (1) (a)(b). A breach of this provision, upon conviction attracts imprisonment for not less than three years without an option of fine and in the case of a continuing offence, a fine of N50, 000 for each day the offence persists.

[46] In 2009, the law was expanded to apply to all websites that have at least 100,000 users per day. In the same 2009, it was reported that China had begun to require websites to collect real names and national identity numbers of those seeking to post comments on the Internet. In both 2007 and 2009, authorities in Malaysia raised the possibility of requiring bloggers to register with the government. In January 2010, a law went into effect in the state of South Australia forbidding anonymous political commentary online, politicians quickly backpedalled in the face of public outcry. Most recently, concerns about cybercrimes and cyber security have prompted calls to limit anonymity, but, so far without consensus on what action is best suited to the problem.

gender, economic power, military force, place of birth. The Internet is also global and open as it is not inhibited by distance – people can communicate on the Internet no matter how far they are separated by distance. Admitted that the Internet is a technology, it therefore means that technical knowledge, tools and methods can be applied to it for the purpose of curbing any negative effects caused by its use. There are three important technical mechanisms that have been identified in this paper, including: state technical control, control by service providers and control by rating, filtering or blocking of access. These three levels of control depict the responsibilities of government itself, the Internet service providers and the Internet users in addressing these quagmires of the amoebic Internet. These technical controls are discussed below.

State Technical Control Approach

This approach may be adopted by governments which believe that they have a right and even a responsibility to intervene directly and place technical controls on the content that can be accessed by their citizens. A classic case is found among the Middle East countries, particularly, Saudi Arabia where all of the country's Internet Service Providers have to go through a central node where the Saudi Arabian authorities block access to sites hosting pornographic materials, those believed to cause religious offences, and web sites containing information on bomb-making. In China, all the Internet cafes are required to keep records of sites visited, with the aim of preventing access to sites featuring pornographic materials, gambling and those that harm national unification, sovereignty and territorial integrity. Prior to an important congress of the Chinese Communist Party in November 2002, the authorities even blocked all access to the Google search engine for a time.[47] In United Arab Emirate, pornographic and religious websites are blocked against public access. Many governments have sought to expand their surveillance powers to online platforms, often without adequate safeguards for user privacy.[48] Such practices, however, can chill online expression and lead to self-censorship on the part of users.

Control by Service Providers

This mechanism rests entirely on initiatives by the Internet Service Providers industry. For example, in 1996, the Internet Service Providers industry in the United Kingdom established the Internet Watch Foundation (IWF) which operates a 'notice and take down' procedure.[49] The Internet Watch Foundation is a registered charity organisation funded by industries and government, which leads some to categorize it as a QUANGO (Quasi NGO). The IWF blacklist is updated twice daily through a two stage process of public complaint and expert review. The Internet Service Providers and software makers use the blacklist to block access to or remove from search results the listed sites. Here, the Internet Service Providers as a group regulate the behaviours of their customers by taking down offensive websites or blocking offensive contents.This mechanism is normally backed by state power and government threat, but the actual implementation and mechanics of the suppression of material is delegated to a trade group made up of the Internet Service Providers as members. The government usually impose liabilities for failure to remove offensive contents by these service providers. However, it is important to note that when the Internet Service Providers come together to regulate certain classes of content in exchange for some limit on their liability for that content, the overwhelming tendency will be to censor more materials, rather than less, in an effort by the Internet Service Providers to be certain that they have removed any material that might be illegal.

Labelling/Rating, **Filtering Techniques and Blocking of Access**

This approach is most especially adopted by parents, guardians, supervisors and teachers who make use of filtering software which alone or in conjunction with the self-rating of sites can limit access by particular users to particular contents of the Internet. Blocking, filtering,[50] and labelling/rating[51] techniques can prevent individuals from using

[47] Other countries where the state is endeavouring to limit access to the Internet by its citizens include Algeria, Yemen, Bahrain, United Arab Emirates, North Korea, Vietnam, Iran, the Maldives and Singapore.

[48] See Privacy International, 'Leading Surveillance Societies in the EU and the World, 2007', available at <https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007> accessed on January 30, 2019.

[49] This procedure involves the vetting of content before publication on the Internet.

[50] Filtering is a technical means of blocking the transfer of certain information considered to be harmful, from one source to the other. This is used especially to prevent children from viewing pornographic content.

the Internet to exchange information on topics that may be controversial or unpopular, enable the development of country profiles to facilitate a global/universal rating system desired by some governments, block access to content on entire domains, block access to Internet content available at any domain or page which contains a specific key word or character string in the address, and over-ride self-rating labels provided by content creators and providers.[52] For example, several countries block access to YouTube.[53] China's extensive system is well documented.[54] Several countries maintain licensing systems that require the Internet Service Providers to block access to certain contents. For instance, India's filtering mandates are imposed, in part, through the Internet Service Providers' license agreements with the Department of Telecommunications.[55] While filtering denies access to certain content, some recent regulations go as far as cutting off the Internet access entirely. Most remarkably, France has adopted a law that provides for cutting off the Internet access of individuals who violate copyright law.[56] And some governments have temporarily cut off or throttled national Internet connections in response to popular unrest as a way to restrict citizen's ability to communicate with each other or the outside world.[57] China has issued rules requiring anyone with the Internet access to refrain from proscribed speech. And the Singapore Broadcasting Authority requires all the Internet Service Providers to abide by licensing terms demanding that they block access to foreign web sites and newsgroups deemed harmful to national morals.[58]

6. Domestic Law and Technology to the Rescue? No, there is Need for a Global Effort

This portion of this paper raises the issue of whether domestic law and technology only are actually rescue agents of the society in addressing these quagmires of the amoebic Internet. First, it should be noted that law and technology are products of the society. Thus, a particular society may decide to have or not have a particular law addressing a particular issue. Also, a particular society may decide to use or not use a particular technology for certain reasons. Besides, the presence of law and technology or their absence in a particular society may depend on the capacity and will-power of that society and its government. This means that, it is possible for a particular country to have the law and technology addressing these menaces of the amoebic Internet while another country may not have. But the phenomenon of the Internet is one that defies the impediment of distance in its operation. The implication of this is that a country without either the law or the technology to circumvent this amoebic nature of the Internet becomes a den of cybercriminals to the detriment of the entire world. This is because a situation of legislative, regulatory and technological arbitrage would be in place. Arbitrage in terms of law and regulation is a very similar process, and consists of locating a commercial activity or part of it in a jurisdiction which confers advantages while continuing to do business in other jurisdictions without being subject to the burdens which those jurisdictions impose on local businesses. Applying this to the Internet, it means that the Internet User can take advantage of the fact that a particular jurisdiction is lacking in policies, technology, regulations and laws against the quagmires of the amoebic Internet by residing therein to carry out illegal activities with impunity whereas the

[51] This is the assessment for value of web sites or online service before connecting to it.

[52] For example, the Open Net Initiative recently reported Microsoft Bing□ s practice of filtering out searches of sexually explicit keywords in Middle Eastern countries, available at <http://opennet.net/sex-social-mores-and-keyword-filtering-microsoft-bing-arabiancountries> accessed on January 30, 2019.

[53] See Open Net Initiative, 'YouTube Censored: A Recent History', available at <http://opennet.net/youtube-censored-a-recenthistory> accessed on January 30, 2019.

[54] Open Net Initiative, 'China's Green Dam: The Implications of Government Control Encroaching on the Home PC', available at <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc> accessed on January 30, 2019.

[55] Open Net Initiative, 'India' (May 9, 2007), available at <http://opennet.net/research/profiles/india> accessed on January 30, 2019.

[56] Nate, A, 'Prepare for Disconnection! French "3 Strikes" Law Now Legal', Ars Technica (October 22, 2009), available at <http://arstechnica.com/tech-policy/news/2009/10/french-3-strikes-law-returns-now-with-judicial-oversight.ars> accessed on January 30, 2019.

[57] See Ronald, D, and Rafal, R, 'Chapter 6: Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet', in *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008), available at <http://opennet.net/sites/opennet.net/files/Deibert_07_Ch06_123-150.pdf> accessed on January 30, 2019.

[58] See Global Internet Liberty Campaign Principles, available at <www.wikipedia.com> accessed on April 05, 2018. Global Internet Liberty Campaign is a group of human rights and civil liberties organisations, its member organisations are spread across the world.

impacts of his actions are felt in other jurisdictions with policies, technology, regulations and laws for addressing the quagmires of the amoebic Internet. In this way, while operating from such jurisdiction without policies, technology, regulations and laws for addressing the quagmires of the amoebic Internet, the Internet User would be perpetrating cybercrimes which their repercussions are felt in jurisdictions with varying legal and technological frameworks to try cybercriminals. By so doing, the Internet User would be operating scot free since his actions are not forbidden in the jurisdiction from where he is operating.

Based on the foregoing, the act of a state putting laws and technologies in place towards addressing the quagmires of the amoebic Internet may not actually exonerate that state from that menace. Because the whole world has not embraced a uniform legal and technological framework for addressing the quagmires of the amoebic Internet, it leaves the non-compliant states open for exploitation by cybercriminals and hinders the effort of compliant states in improving the worldwide enforcement of transnational cybercrimes. The Internet is, in a remote sense, analogous to a 'common heritage of mankind.'[59] No one owns it, people of all nationalities use it and experience all the challenges emanating from its use. This makes the issue of addressing the quagmires of the amoebic Internet a global one. Any effort towards addressing the quagmires of the amoebic Internet must not be left within the bounds of domestic jurisdiction. There must therefore be a globally galvanized mechanism to achieve success.

7. Conclusion

There is need for applying best practices and educating everyone who is legitimately using the Internet about safe use. The amoebic nature of the Internet has made it easier for cybercriminals to steal information remotely. The government will need to interface with ordinary citizens engaging online on protection awareness and safety consciousness. Learning materials, security tools and tips should be articulated, localized and transmitted online to safeguard the most critical assets of the global people. Governments and organisations need to find incentives to get cooperation from private corporations and to promote and support international cooperation, especially through international organisations such as International Telecommunications Union. Every nation should also participate in working groups of its international and regional partners to ensure a harmonization of efforts, particularly in the area of legislation. The main task of the international legal regulation in this sphere is organisation of cooperation between the states and coordination of their efforts in global exchange of information. The Internet is a super highway which anybody can ply anytime, and just like law can regulate the movement of people and goods that pass different routes especially while crossing borders (subjecting same to verification, quarantine, vaccination and other scrutiny), so should the product of the Internet be verified before making same available. This will be helpful in getting rid of some cybercrimes even before their occurrence. There is no doubt that these quagmires have become an image nightmare for the world due to the opportunities presented by the amoebic Internet. Cybercriminals may shut down the world with the click of a button and what could we then do? So, it is imperative that an international coalition addressing the quagmires of the amoebic Internet is formed and that a global treaty is enacted to harmonize domestic laws and technologies in order to protect the vulnerable infrastructures and the citizens of the world. Since the Internet itself is a technological phenomenon, there is no doubt that the best way to handle these quagmires is through a technological approach backed by law.

[59] This phrase was coined by Antonio Segura-Serrano in his work, Internet Regulation and the Role of International Law. See Antonio S, 'Internet Regulation and the Role of International Law' in A V Bogdandy & Wolfrum (eds) *Max Planck Yearbook of United Nations Law* (Netherlands: Kininklijke Brill N. V., 2006) vol. 10, pp. 231 – 260.