UNIVERSITY OF BENIN LAW JOURNAL

UBLJ (2018) Volume 18 No. 1 ▪ ISSN 1117-8035

THE NEED FOR REGULATION OF THE INTERNET TECHNOLOGY TOWARDS ENSURING NATIONAL SECURITY

Kenneth Uzor EZE, PhD*
Iloh Friday OKECHUKWU, LLM*

Abstract

The Internet technology is creating a world that is both everywhere and nowhere, but it is not where living beings live. It is creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or place of birth. It has created a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. This nature of the Internet technology has necessitated a call for regulation of the technology towards ensuring national security. Using doctrinal method of research, this paper therefore considers the various forms by which this technology called 'the Internet' could be regulated to engender national security. There is no gainsaying that throughout history, there is no phenomenon that is devoid of regulation and the Internet technology cannot be any exception. This study reveals that if anarchy reigns supreme in the use of the Internet technology, then, the essence of the Internet itself will be defeated. It has been found out that the problem of uncertainty of regulatory platform is still a huge challenge towards achieving effective regulation. This paper concludes that freedom on the Internet should not be entirely free as far as the Internet use is concerned because the purported freedom on the Internet is now increasing the wave of cybercrimes with the resulting adverse effect on national security as it affects vulnerable infrastructures and national cum global economies, hence, this need for regulation of the Internet technology to engender national security.

* Kenneth Uzor Eze (LL.B, BL, LL.M, MIAD, PhD, PGDIT,pnm) Lecturer, Faculty of Law, Nigeria Police Academy, Wudil Kano, Nigeria. E-Mail: skennue@yahoo.com. Phone No.: 080868686518.

*. Iloh, Friday Okechukwu (LL.B, BL). Law Teacher, Faculty of Law, Ebonyi State University, Abakaliki, Ebonyi State, Nigeria. E-Mail: ilohfriday@gmail.com. Phone Nos: 08061527156, 08056436125.

1.0. Introduction

The Internet technology now consists of transactions, relationships, images, programmes, thoughts, and other activities arrayed like a standing wave in the web of our communications. The legal concepts of property, physical expression, identity, movement do not apply to the Internet technology. Those concepts are based on matter, but there is no matter in the Internet. Sequel to all these, arguments abound with respect to regulation of the Internet technology. But much as people would like to see some forms of regulation of the Internet use, most people are at the same time not sure how it can be done. However, this is not an argument that regulation is impossible but one as to the difficulty or the blurred nature of the issues relating to regulation of the Internet technology. As shall be seen below, there are reasons which account for the Internet regulation and other reasons which stand against regulation of the Internet technology. The analyses of these two sides of the coin will reveal that it would be preferable to regulate the Internet use than sacrifice same on the altar of the Internet freedom to the detriment of innocent users of the Internet. Such regulation of the Internet technology will, no doubt, engender national security.

1.1. Conceptualization: Setting the Limits

We shall proceed in this discussion with the conceptual clarification of the key terms in this paper. These key terms include; the Internet, regulation of the Internet technology, national security.

1.1.1 Defining the Internet

As shall be seen below, there have been some attempts to define this technology called the Internet. However, the Internet has not really confined itself to a particular definition. According to Ashaolu and Oduwole, 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. The Internet is the large system of connected computers around the world which allows people to share information and communicate with each other.[4] At best, this technology

[3] Ashaolu David and Oduwole Abiodun, *Policing Cyberspace in Nigeria* (Nigeria: Life Gate Publishing Co. Ltd. 2009), 3.

[4] See generally, Eze Kenneth Uzor, "A Review of the Problems in Regulating the Internet Use: Enforcement Mechanisms against Cybercrimes under International Law" (PhD thesis, Nnamdi Azikiwe University, 2016), 38 – 43.

called the Internet can only be described. Accordingly, it can be described as an electronic network which may be wired or wireless by which one can transmit and receive data with the use of a computer system. An Internet communication system consists of interconnected packet networks supporting communication among host computers using the Internet protocols. The networks are interconnected using packet-switching computers called 'gateways' or the 'Internet protocol routers' and intermediate systems.[5]

1.1.2 Regulation of the Internet Technology

Regulation of the Internet implies controlling the use of the Internet technology to ensure that illegal and wrongful contents are not freely created, distributed and accessed by the netizens.[6] Today, almost everything done in the physical are presently being conducted on the Internet such that much of the threats presently against national security are conducted on the Internet. Sequel to this, the level of security required in the physical should be replicated on this virtual phenomenon of the Internet technology. The need for regulation of the Internet technology, therefore, cannot be over-emphasized. Thus, the freedom on the Internet should not be entirely free as far as the Internet use is concerned because the purported freedom on the Internet is now increasing the wave of cybercrimes with the resulting adverse effect on vulnerable infrastructures and national cum global economies. It is important to state here that the forms of regulation featured in this paper do not dwell deeply on computer engineering and technical standards relating to the Internet regulation, but deal more with the legal angle. Reference may however be made to technical standards where necessary.

1.1.3 National Security

National security is a concept that a government should protect the state and its citizens against all kinds of national crises through a variety of power projections, such as political power, diplomacy, economic power, military might, and so on. By and large, national security presupposes the capability of the government of a state to protect the state and its citizens against all kinds of national crises by overcoming the multi-dimensional threats to the apparent well-being of its people and its survival as a state at any given time. Some of these threats, no doubt, are known to have emanated from the use of the Internet technology, hence, the need for regulation of the Internet technology to engender a stable national security.

---

[5] *Ibid.*

[6] Netizens simply means the Internet users.

1.2. Arguments for Regulation of the Internet Technology

The reasons canvassed for regulation of the Internet technology include:

1.2.1 The Internet should be Regulated like other Electronic Networks

The argument here is that, notwithstanding the unique complexities of the Internet technology, it remains an electronic data delivery and reception mechanism. In that sense, it is not fundamentally different from other electronic communications networks such as radio, television and telecommunications. These other networks are regulated and so should the Internet. If broadcasting and telecommunications are the subject of very different regulatory regimes, the Internet should similarly have its own distinctive system of regulation.

1.2.2 There are Harmful and Offensive Contents on the Internet

The rate of pornography of all kinds on the Internet is alarming. The major problem here is child pornography and sexual solicitation of children. Victims of pornographic contents have suffered grievous harms and embarrassments. That being the case, people entrusted with responsibility for children such as parents, guardians and teachers will want to place some limitations on access to pornographic materials made available on the Internet, thereby favouring regulation of the Internet technology.

1.2.3 Criminal Activities Often Take Place on the Internet

The Internet users see it as powerful mechanism for transferring and receiving all sorts of information and for conducting commercial activities. These good sides of the Internet, notwithstanding, some people use it for a wide range of negative activities constituting cybercrimes. These include copyright theft, credit card fraud, financial scams, money laundering, hacking, industrial espionage, cyber terrorism, actual terrorism, bomb making instructions, prostitution, certain forms of gambling, drug use, drug smuggling, suicide assistance, defamatory allegations, cyber stalking, etc. Thus, victims of these crimes would support regulation of the Internet technology to control or put an end to these crimes

1.2.4 The Internet is Global and Open to Everybody

The idea of the Internet technology emerged as a result of the need to expeditiously exchange research results among top research institutions in America in response to the pressures of the cold war period. It started with the American military establishment; then it was broadened to the American academic community; next, it grew to academic communities in

other industrialised countries; now the Internet has users in every country and among virtually all age groups. There were probably some rules on use of the Internet technology before it went 'public', but certainly there was no formalised regulation as there was no need for that by then. Today, the Internet can be accessed by any person from the privacy of his or her bedroom at any time of the day or night. This global and open nature of the Internet, therefore, gives rise to the need to put in place some mechanisms for allowing the final user to determine and control what is accessed on the Internet.

1.2.5 There should be Some Form of Control or Regulation of the Internet

Most governments, politicians, the Internet Service Providers as well as institutions and organisations, especially those that have been negatively affected by the Internet use, all favour some forms of regulation of the Internet. In taking this view, it is clear that they are reflecting the wishes of consumer groups and users themselves.

1.3. Arguments against Regulation of the Internet Technology[7]

The reasons canvassed against regulation of the Internet technology include:

1.3.1 The Global Nature of the Internet Technology

It is argued that, quite unlike other communications networks, the Internet technology is simply enormous, growing rapidly and genuinely global and that, in these circumstances, even if one wanted to, it is just not possible to regulate the Internet. This cannot, however, be an argument as to why regulation is undesirable but one as to why it is difficult and the fact that something is difficult does not mean that it is impossible or should not be done. For example, before the coming into place of the Convention on the Law of the Sea, 1982,[8] it was so problematic how to regulate activities in the seabed and ocean floor and its resources. But, under the 1982 Law of the Sea, an International Seabed Authority was established to administer the access to, and exploitation of the seabed area.[9] Even the use of the outer space and the Antarctica was very contentious until the emergence of the 1959 Antarctic Treaty[10] and the 1967 Outer Space Treaty,[11]

---

[7] *Ibid.*

[8] UN Doc. A/CONF. 62/122: (1982) 21 I. L. M. 1261.

[9] UN Doc. A/CONF. 62/122; art. 1(1), 136.

[10] U. K. T. S. 97 (1961), Cmnd. 1535, 402 U. N. T. S. 71. Treaty came into force in 1961 with 46 parties, including United Kingdom.

[11] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, January 27, 1967, 18 U. S. T. 2410, U. N. T. S. Vol. 610, No. 8843.

respectively. Why should the case of the Internet technology be different? If the international community comes up with any mechanism at all, which must not necessarily be in line with what is now adopted in respect of the seabed and ocean floor, outer space, and Antarctica, why would the Internet technology not be regulated? Or is the whole world ready to face the whole lots of consequences that will accompany such state of anarchy on the Internet use, if left unregulated?

1.3.2 Infringement on the Right to Freedom of Expression

It is argued that any system of control of content of the Internet represents a breach of the individual's right to freedom of expression on the Internet and that such a right is absolute and cannot be qualified without irreparable damage to civil liberty in a free society. In any event, all rights have to be qualified because absolute rights threaten other rights. For example, an unrestricted right to freedom of expression and press on the Internet by which pornographic contents exist on the Internet would threaten the right of children to be free from abuses, molestations and embarrassments. Also, it should be noted that fundamental right may be qualified on the basis of public safety and order, etc.[12]

1.3.3 The Internet is Different in Operation from other Communications Networks

It is argued here that there is no need to regulate the Internet technology because its use is quite different from other communications networks. Whereas radio and television is pumped into millions of homes simultaneously (push technology), the Internet is an interactive medium and requires a particular user actively to seek a particular site or application (pull technology). In fact, this difference in operation of the Internet technology is an argument for its regulation and not an argument against its regulation. For example, because radio and television are mass media, there are limits to the amount of sex and violence-related issues that will be permitted through them but the Internet technology, as liberal as it is, should be subjected to some controls and checks to avoid anarchy online.

---

[12] For example, section 45 (1) of the *Constitution of the Federal Republic of Nigeria*, 1999 (as amended) provides that nothing relating to the right to private and family life, right to freedom of thought, conscience and religion, right to freedom of expression and the press, right to peaceful assembly and association and right to freedom from discrimination shall invalidate any law that is reasonably justifiable in a democratic society – (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom of other persons.

1.3.4 The Internet is Different in Kind from other Communications Networks

It is argued here that the genesis of the Internet technology was such that it embraced and fostered a new spirit of freedom, openness and experimentation and that these values must remain an integral feature of the Internet. At best, this view is simply erratic. The Internet is now a fundamentally different operation than the days before the arrival of the World Wide Web and mass usage of the medium. Now many users are accessing many websites and, in that circumstance, there are contents and there are activities that require some forms of regulation. At worst, this view is anti-commercial and prone to encouraging cybercrimes. The reality is that the overwhelming bulk of the Internet's infrastructure is now owned and operated by private corporations and there is an explosive demand for e-commerce services. Having made the above points, the next sub-heading will deal with some forms of regulation of the Internet technology towards ensuring national security. These forms of regulation captured mainly the national standard for ensuring national security.

1.4. Some Forms of Regulation of the Internet Technology

Despite its unique qualities, the Internet technology remains inaccessible to a large percentage of the world's population. The openness, abundance and relative inexpensiveness of the Internet are largely irrelevant to those struggling for daily survival. Issues as fundamental as access to electricity, pose barriers to many. Nevertheless, the Internet has grown much faster, reached far more people, and become far more critical to economic activities and human developments than any other medium in history. However, the freedom of expression on the Internet is not guaranteed by this technology.[13] Not even its open architecture is assured. While the Internet technology can operate without gate-keeping, it has nodes that can become checkpoints. While it is designed to be global and borderless, it is vulnerable to national controls. The very power of the Internet's technology is double-edged: networked technologies can enable the exercise of rights, or be used by governments to exert greater control. Despite the power of the Internet technology to facilitate communication and promote democracy, or perhaps because of that very power, governments are becoming increasingly aggressive in trying to restrict the Internet. Government efforts to limit freedom of expression online are taking many forms. There are five basic approaches to regulation of the

[13] See William H. Dutton, Anna Dopatka, *et al*, "Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet," last modified August 19, 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1654464.

Internet technology. These approaches are by no means mutually exclusive as different countries are giving different emphasis to different approaches. These approaches include:

1.4.1 Constitutional Approach

This approach makes the Constitution of the country the prime determinant of what is 'acceptable' on the Internet. Classically, this has come to be the United States of America's approach as efforts to enact relevant legislations for regulation of the Internet use have fallen foul of the United States Constitution, in particular the first amendment on freedom of expression. For example, in *Reno v ACLU,*[14] the case involved a challenge to the Federal Communications Decency Act, which 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. The United States Supreme Court declared the Federal Communications Decency Act unconstitutional. This case explored the unique features of the Internet technology as they relate to the legitimacy of government controls using this constitutional approach

1.4.2 State Technical Control Approach

This approach is 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 offence, 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.[15] 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

---

[14] *Reno v. American Civil Liberties Union*929 F. Supp. 824, 830 - 849 (E. D. Penn. 1996). The Supreme Court decision is available at http://www.law.cornell.edu/supct/html/96-511.ZS.html.

[15] 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.

without adequate safeguards for user privacy.[16] Such practices can chill online expression and lead to self-censorship on the part of users.

1.4.3 Statutory Approach

This approach makes a specific piece of legislation the prime determinant of what is 'acceptable' on the Internet. Laws pre-dating the Internet can be invoked to restrict expression online, sometimes with global reach or with implications unanticipated when the laws were enacted. For example, a lawsuit in France against Yahoo for providing access to Nazi-related material created and hosted in the United States of America did not require enactment of a new law, but merely the application of existing French laws.[17] Also, some governments have specifically criminalized certain types of content on the Internet. Such laws may be intended, for example, to protect minors from materials regarded as 'harmful', but they end up limiting the access of all users, both minors and adults, to otherwise lawful material. For instance, the United States adopted the Communications Decency Act and the Child Online Protection Act in an attempt to protect children from inappropriate content.[18]

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.[19] 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.[20] 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.[21] Again in Nigeria, under the Advance Fee Fraud and other Fraud Related Offences

---

[16] Privacy International "Leading Surveillance Societies in the EU and the World, 2007," https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007, (accessed April 20, 2016).

[17] See generally, Centre for Democracy and Technology, "'Regardless of Frontiers': the International Right to Freedom of Expression in the Digital Age," *Version 0.5 – Discussion Draft* (April 2011) 8, www. Cdt.org. (accessed February 22, 2017).

[18] *Ibid.*

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

[20] Aaron Morris, "South Korea Passes Cyber Defamation Law," Internet Defamation Blog, last modified May 4, 2009, http://internetdefamationblog.com/tag/cyber-defamation-law/, accessed April 20, 2016.

[21] *Egypt Telecommunication Regulation Law, Law No. 10 of 2003*, art. 64.

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.[22] Moreover, any person or entity who in normal course of business provides telecommunications or 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.[23] South Korea requires websites to obtain users' real names and national identity numbers before posting any comments or uploading any user-generated content.[24]

1.4.4 Self-Regulation Approach

In the European Union and in a number of other countries, 'self-regulation' has been offered as a viable alternative to governmental control of the Internet content. This approach is supposed to rest entirely on voluntary 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.[25] 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

---

[22] *Advance Fee Fraud and Other Related Offences Act, 2006,* Cap. A6. Laws of Federation of Nigeria, 2011, s.12.

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.

[23] *Advance Fee Fraud and Other Related Offences Act,* s. 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.

[24] 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.

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

expert review. The Internet Service Providers and software makers use the blacklist to block access to or remove from search results the listed sites.

Thus, the use of the term 'self-regulation' is a misnomer in the context of controlling speech on the Internet. In the normal sense of the phrase, 'self-regulation' is when a group of people or companies decide that, in their own best interest, they should themselves regulate how they go about their joint interests. However, what is being suggested by the term 'self-regulation' as applicable to the Internet technology is not that the Internet Service Providers as a group should regulate their own behaviour, but rather that the Internet Service Providers should regulate the behaviour of their customers by taking down offensive websites or blocking offensive content.

Here, privatized control may be harder to challenge. However, in a number of cases, it may be clear that the Internet Service Providers is acting under pressure from the government and has, in essence become the agent of the government for carrying out a government policy. What is often promoted as the Internet 'self-regulation' is actually 'privatized censorship'. It is consistent with the fairly common occurrence of having a formerly direct government function turned over to a private business. The backing is still state power and government threat, but the actual implementation and mechanics of the suppression of material is delegated to a trade group.If it can be shown that 'self-regulatory' measures are mere proxies for more direct government control, they may be vulnerable to challenge under human rights law. When the Internet Service Providers come together to self-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.

1.4.5 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,[26] and labelling/rating[27] techniques can prevent individuals from using the Internet to exchange information on topics that may be controversial or unpopular, enable the development of country profiles to facilitate a

---

[26] 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 specially to prevent children from viewing pornographic content.

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

global/universal rating system desired by some governments, block access to content on entire domains, block access to the 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.[28] For example, several countries block access to YouTube – by 2008, more than half a dozen countries, including Brazil, China, Syria, Thailand, Pakistan, and Turkey had blocked the YouTube platform temporarily or otherwise.[29] China's extensive system is also well documented.[30] In the United States of America, regulation of the Internet dwells more on human rights protection, particularly the right to freedom of expression and speech on the internet, especially as everything about the Internet relates to expression. The Supreme Court case of *Reno v ACLU*[31] is an eye-opener. The case involved a challenge to the Federal Communications Decency Act, 1996[32] which sought to protect children from harmful internet materials 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. In a historic ruling, by a majority of seven against two, the United States Supreme Court declared the impugned provisions unconstitutional and as vague and overbroad, holding as follows:

> As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that Government regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven of censorship.

---

[28] For example, the Open Net Initiative recently reported Microsoft Bing' s practice of filtering out searches of sexually explicit keywords in Middle Eastern countries, http://openinet.net/sex-social-mores-and-keyword-filtering-microsoft-bing-arabjancountries. (accessed April 15, 2016).

[29] Julian York, "A Brief History of YouTube Censorship," last modified March 26, 2018. https://motherboard.vice.com/en_us/article/59jgka/a-brief-history-of-youtube-censorship. See also, Open Net Initiative, "YouTube Censored: A Recent History," last modified April 15, 2016, http://opennet.net/youtube-censored-a-recenthistory.

[30] Open Net Initiative, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc. (accessed April 15, 2016).

[31] *Reno v American Civil Liberties Union*, 929 F. Supp. 824, 830 - 849 (E. D. Penn. 1996). The Supreme Court decision is available at http://www.law.cornell.edu/supct/html/96-511.ZS.html. (accessed February 2, 2013).

[32] The Act generally made it illegal to transmit indecent and obscene material on the internet.

In 2006, the United States Department of State launched the Global Internet Freedom Task Force (GIFT). The GIFT's main foreign policy objective is enhancing global internet freedom by monitoring human rights abuses and enhancing access to the internet through technical and financial support for increasing availability in the developing world. A form of expanding access to the internet is to create mirror sites that serve as alternatives to websites that are blocked in some countries, or to develop tools and instructions that enable users to work around a country's firewalls.[33] In the United States of America, apart from freedom of expression on the internet, anonymity on the internet is also encouraged. Federal and state courts have found that the first amendment to the United States' Constitution protects the right to speak anonymously on the internet.[34]

While filtering denies access to certain content, some recent regulations go as far as to cut 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.[35] 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.[36] 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

---

[33] The International Strategy for cyberspace and global internet freedom initiatives present a very different view of cyberspace from the United States Department of Defence's doctrine, which emphasizes full spectrum dominance and cyberspace as an operational, war-fighting domain. A question exists about the definition of sovereignty in cyberspace. Although no one country 'owns' cyberspace, each may have the authority to regulate its portion of the internet, similar to territorial waters or airspace. What constitutes computer-based crime may be determined by domestic standards, and one country's internet freedom initiative may be another country's cybercrime.

[34] See, *Solers Inc. v Doe*, 2009 D. C. App. LEXIS 342 (D. C. Cir. 2009); *Doe v Cahill*, 884 A. 2d 451 (Del. 2005).

[35] Nate Anderson, "Prepare for Disconnection! French '3 Strikes' Law Now Legal,"ArsTechnica, last modified October 22, 2009, http://arstechnica.com/tech-policy/news/2009/10/french-3-strikes-law-returns-now-with-judicial-oversight.ars. (accessed April 15, 2016).

[36] See Ronald Deibert and Rafal Rohozinski, "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). http://opennet.net/sites/opennet.net/files/Deibert_07_Ch06_123-150.pdf. (accessed April 17, 2016).

they block access to foreign web sites and newsgroups deemed harmful to national morals.

1.5. Findings

Notwithstanding the quantum of argument in favour of the Internet regulation, it is still not certain which regulatory platform should be in charge of regulation of the Internet. The result could well be total confusion and obscurity in regulation of the Internet technology because there will be conflict or lack of clarity of regulatory powers. Besides, the implication of foreign Internet Service Providers for Nigeria's security is also an issue. This raises the question of whether these foreign Internet Service Providers may be subjected to Nigeria's jurisdiction for the purposes of ensuring national security. Therefore, in an attempt to control the activities on the Internet especially as it concerns what citizens may access on the Internet, there is the question of whether a foreign Internet Service Provider that sends data through the Internet may properly be forced to follow the laws or defend itself in court in any forum in which the data can be accessed on the Internet?

National governments have maintained that they have the right to regulate the activities of the Internet Service Providers operating from within the boundaries of another sovereign nation. In the United States' State of Minnesota for instance, the Attorney General's office posted a warning that 'persons outside of Minnesota who transmit information via the Internet knowing that the information will be disseminated in Minnesota are subject to jurisdiction in the courts of Minnesota for violation of state criminal and civil laws.'[37] By and large, in Nigeria, under the Advance Fee Fraud and other Fraud Related Offences Act, 2006, a duty of care is imposed on the service providers to ensure that their services and facilities are not utilised for unlawful activities.[38]

1.6. Recommendations

First and foremost, there should be more emphasis on the responsibility and not the liability of the Internet Service Providers in regulation of the Internet technology. This means that instead of wasting much energy on checkmating the Internet Service Providers for their online contents, more attention should be given to fashioning out ways of getting these Internet Service Providers more involved in executing technical standards for ensuring a safe Internet use. This can be achieved by making the Internet Service Providers to figure out their own border control systems. In this

---

[37] See Nandan Kamath, *Law Relating to Computers Internet and E-Commerce* (India: Universal Law Publishing Co. Pvt. Ltd., 2014), 275.

[38] *Advance Fee Fraud and Other Related Offences Act*, s.13 (3).

sense, there should be an effective collaboration between law enforcement agencies and the Internet industry which must be legally regulated by imposing duty on the Internet providers to ensure data storage, identification and information thereby shifting protection from providers to individual users. This is because it is by being responsible that liability is nabbed in the bud. For example, in Nigeria, a duty of care is legally imposed on the Internet Service Providers to ensure that their services and facilities are not utilised for unlawful activities.[39]

Secondly, the greatest problem bedevilling the Internet regulation is the amoebic nature of this technology called the Internet, which defies localization of conduct and effects. And this problem can also be tackled by a tripartite means or approach including constant review of laws relating to the Internet technology, constant follow up of emerging technology and constant public awareness. There should be proper and adequate sensitization about the Internet technology to beat the problem of arachnophobia on the web.[40]

Thirdly, regulation of the Internet technology, whether at the national or international level should be assigned to a clearly defined body to avert the above articulated challenge of uncertainty of regulatory platform.

1.7. Conclusion

National security was initially thought to focus only on military might but has been understood to encompass a broad range of facets, all of which impinge on the non-military or economic security of the nation and the values espoused by the national society. Accordingly, in order to possess national security, a nation needs to possess economic security, energy security, environmental security, on-line security, etc. This is because security threats involve not only conventional foes, but events and phenomena causing insecurity and severe damage in this category. Today, virtually everything done in the physical are presently being conducted on the Internet such that much of the threats presently against national security are conducted on the Internet. Sequel to this, the level of security required in the physical should be replicated on this virtual phenomenon of the Internet technology. The need for regulation of the Internet technology, therefore, cannot be over-emphasized. Thus, the freedom on the Internet should not be entirely free as far as the Internet use is concerned because the purported freedom on the Internet is now increasing the wave of

---

[39] *Advance Fee Fraud and Other Related Offences Act*, part II, s. 13 (3).

[40] Arachnophobia on the *web* means the fear of dealing with or operating the computer due to what might be the outcome. See Nandan Kamath, *Law Relating to Computers Internet and E-Commerce* (India: Universal Law Publishing Co. Pvt. Ltd., 2014).

cybercrimes with the resulting adverse effect on vulnerable infrastructures and national cum global economies. Regulation of the Internet would bring about resilience of national critical infrastructure, as well as detect and defeat or avoid threats and espionage against classified information. Finally, regulation of the Internet permissible must simply be useful, reasonable or desirable, hence required by a compelling government interest. The least restrictive means test which holds that, when there are several options for accomplishing an objective, the other least restrictive to the right of free expression must be chosen. Thus, the restriction of free expression on the Internet must be closely tailored to the accomplishment of the legitimate objective necessitating it. Censorship should be directed against clearly illegal content and not content which had not been adjudged defamatory because of the risk of over blocking.