THE INTERNET AND ITS FACILITY FOR CRIMINALITY: SOME UNIQUE DIFFICULTIES FOR INVESTIGATION AND PROSECUTION[1]

Abstract

This study examines critically the nature of the Internet in relation to its facility for committing crimes. It discovers that the Internet is open, user-controlled, global, decentralized, inexpensive, abundant, interactive, and makes use of independent infrastructure. All these features are combined to form the medium's transnational nature that challenges ordinary traditional regulatory platforms. It is also found that with increasing over dependence on computer systems within the global Internet network, the incidence of cyber criminality is significantly on the rise. Yet, the processes of investigation and prosecution of suspects are greatly hindered as a result of the amoeboid nature of cyberspace which makes it difficult to locate suspects and their conducts. The paper advocates progress in more sophisticated technology that would aid easy identification of suspects, constant review of cyber laws, and increased public enlightenment on the operations of the Internet. Doctrinal and critical approaches were employed in the study.

Key words: *The Internet, Cyber criminality, Investigation, Prosecution, Jurisprudence, Cyber Law*

1. Introduction

The development of the Internet is traceable to the cold war times when there arose a need to establish link among the top universities of the United States of America to enable them to expeditiously share the fruits of their research.[2] This effort followed the establishment of Advanced Research Project Agency (ARPA) in 1950s immediately after the era when Russians climbed the space with the launch of a sputnik. When the ARPA succeeded in 1969, it did not take the experts long to understand how much potential that interconnection tool had. In 1971, Ray Tomlinson made a computer system to send electronic mail. This was a big step in the making of the Internet, as this opened gateway for remote computer accessing called telnet.[3]

In the course of time, rigorous paper works were done in all the leading research institutions. The research continued by giving every computer an address to setting out the rules, while everything was recorded. The year 1973 saw the preparations for the vital Transmission Control Protocol/Internet Protocol and Ethernet Services.[4] At the end of 1970s, Usenet group had surfaced. By early 1980s, IBM came up with its personal computer based on Intel 8088 processor which was widely used by students and universities because it solved the purpose of easy computing. By 1982, the defence agencies made the Transmission Control Protocol/Internet Protocol compulsory and the term 'Internet' was coined. The domain name services arrived in the year 1984 which was also the time when various Internet based services marked their debut.[5]

As the Internet was coming out of its incubation period which took almost two and half decades, the world saw the first computer mishap that was not at all a part of planned strategy. In 1986, a worm or a rust of the computers, Pakistani Brain, the oldest virus created under unauthorized circumstances, infected IBM computers, attacked and disabled over ten percent of the computer systems all over the world. After many break-ins into government and

[1]By **Ikenga K.E. ORAEGBUNAM, PhD (Law), PhD (Phil.), PhD (Rel. & Soc.), MEd, BL,** Senior Lecturer and Ag Head, Department of International Law & Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria. E-mail: ik.oraegbunam@unizik.edu.ng. Phone Number: +2348034711211; and **Kenneth U. EZE, LLB, LLM, BL, PhD Candidate,** Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria.

[2] See generally <www.wikipedia.org> accessed on June 02, 2014.

[3] Ibid.

[4]See also Simple Mail Transfer Protocol(SMTP) and Network News Transfer Protocol (NNTP).

[5] <www.wikipedia.org> accessed on June 02, 2014

corporate computers, the United States Congress passed the Computer Fraud and Abuse Act 1988, making this a crime. The law did not, however, cover juveniles, who are hugely involved in hacking activities. While most of the researchers regarded it as an opportunity to enhance computing as it was still in its juvenile phase, quite a number of computer companies became interested in dissecting the cores of the malware which led to the formation of Computer Emergency Rescue Team (CERT) in 1987.[6] Soon after the world got over the computer worm, World Wide Web came into existence. World Wide Web was seen as a service to connect documents in websites using hyperlinks. It was discovered by Tim Berners-Lee.[7]

By 1990s, the malware had started coming out as more than forty million computers had been sold out, yet antivirus had already been discovered and the graphical user interface was quite in its evolution. 'Archie', the first Internet search, marked the beginning of a new era in the Internet computing. Categorising the websites was in its most dynamic phase and commercialized e-mail sites were developed. It was during this time that the term 'spam' was coined, which referred to fake emails or hoaxes. In 1992, the Internet browser called 'mosaic' came into existence. Another Internet browser, Netscape Navigator, made its debut in 1994 and was later competing with Microsoft's Internet Explorer. By this time, the domain name registration had started to get exponential and was made commercial. In fact, the Internet explosion had started to occur. Coming years saw the launch of giants such as Google, Yahoo as well as strengthening of ultimate revolution creators i.e. Microsoft, Google, IBM, etc.[8]

There is no gainsaying that the emergence of the Internet and the development of computer technology have added a great deal to the quality of human life in the contemporary world. The Internet today touches every aspect of human life irrespective of location in the globe. Thanks to the computer and the Internet, the prophecy of McLuhan[9] as far back as the 1960s about the world becoming 'a global village' is all the more fulfilled today with precision. Hence, the contemporary world is knitted together not just as 'global village' but more aptly as a 'global sitting room', so to speak. Daily activities of human beings are increasingly affected in form, size, content and time by the computer and the Internet in quite positive way. The result is that the benefits of the attendant information revolution are very well extended to all. Banking, commerce, contract, communication, publication, education, research, marketing and so on, are enhanced and facilitated by computer technology and its products.

As advancement in information and communication technology (ICT) has led to the representation of different types of information in electronic format, texts, pictures and voice can all be digitized. Akomolede notes that, for instance, 'many difficulties which hampered international and even national commercial transactions in the past have now been consigned to the dust-bin of history'.[10] Along with these geometric changes in information presentation and distribution are tandem demands in user expectations for more rapid, open and global access to information than has been available in the past. In recent times, with the explosion of GSM telephony services in Nigeria, which saw many networks upgrading their services, social media like Facebook, WhatsApp, and Twitter overnight became commonplace. With billions of people on Twitter, Facebook, LinkedIn and others, trillions of words and billions of images

[6] *Ibid.*
[7] *Ibid.*
[8] *Ibid*.
[9] http://www.marshalmclutianspeaks.com/Last visited on 20-06-14.
[10] T. I. Akomolede, "Contemporary Legal Issues in Electronic Commerce in Nigeria", *Potchefstroom Electronic Law Journal***,** 2008 (3). Retrieved from http://www.ajol.info/index.php/pelj/article/view/42234/9353. Last visited on 30 -06 – 14.

are flying through cyberspace every second as multitudes communicate, chatting, sending SMS and MMS.

Be that as it may, the advent of the Internet and the proliferation of digital regime have also created new opportunities for those who engage in illegal activities. Among these illegalities, criminality occupies the prime position. Magnin observes that 'during the last twenty years, smart computer users using their machine to commit crimes have fascinated the world and generated a strange feeling composed of admiration and fear'.[11] Hence, the sophistication in technology, cybernetics and computer communication has not only produced a dramatic increase in the incidence of criminal activities but has also resulted in the evolution of what seems to be new varieties in criminality. Certainly, old forms of crimes such as fraud, gambling, piracy, forgery, cheating, terrorism, criminal defamation, stealing, and the like, receive more boost and fillip as a result of the speed, convenience and worldwide coverage of the Internet. More still, new types of offences like electronic mail scams, cyber stalking, page jacking, salami attacks, Internet time theft, electronic mail bombing and spoofing, unauthorized access to computer systems or network, and so on, are created and aided by same qualities. The thrust of this study is to discuss the features of the Internet that make it possible and easy for crime to thrive via that medium. The paper also highlights the associated difficulties encountered in the investigation and prosecution of suspected offenders.

2. Conceptualisations: Setting the Limits

2.1. The Internet and Online Services

Unlike online services, which are centrally controlled, the Internet is decentralized by design. Online services are managed by its owners generally called online service providers. Examples of online service providers include blog platforms, e-mail service providers, social networking websites, and video and photo hosting sites. On the other hand, each Internet computer, called a host, is independent; its operators can choose which Internet services to use and which local services to make available to the global Internet community. There are varieties of ways to access the Internet apart from the services provided by the online service providers. Most online service providers offer access to some Internet services such as providing platforms for blogging, e-mail and chat services, hosting of video and photographs, etc. It is also possible to gain access through a commercial Internet service provider or any other Internet intermediary such as mobile telecommunications providers, website hosting companies, etc.

2.2. The Internet and Cyberspace

The word 'cyberspace' is traceable to the Canadian science-fiction writer, William Gibson, who coined the term in his 1982 short story, 'Burning Chrome', but who later described it in his 1984 novel, 'Neuromancer' as 'consensual hallucination…graphic representation of data abstracted from every computer…unthinkable complexity'.[12]Cyberspace is an imaginary, intangible, virtual reality realm where (in general) computer communications and simulations and (in particular) Internet activity take place. As an electronic equivalent of human psyche (the 'mindspace' where thinking and dreaming occur), cyberspace is the domain where objects are neither physical nor representations of the physical world, but are up entirely of data manipulations and information.[13]

[11] C.J. Magnin, *The 2001 Council of Europe Convention on Cyber-Crime: An Efficient Tool to Fight Crime in Cyber-Space*, LL.M Dissertation Santa Clara University, June 2002, p. 1. Retrieved from http://www.magnin.org/publications/2001.06.scu. Last visited on 01-08-14.
[12] Available at www.wikipedia.org accessed on March 29, 2014.
[13] *Ibid.*

Cyberspace is a metaphor for describing the non-physical terrain created by computer systems.[14]Like physical space, cyberspace contains objects such as files, mail messages, graphics, etc., and different modes of transportation and delivery. Unlike real space, though, exploring cyber space does not require any physical movement other than pressing keys on a keyboard or moving a mouse.[15]As noted by Brenner, cyberspace 'is not a fixed, predetermined reality operating according to principles and dynamics that cannot be controlled or altered by man. The cyber world is a constructed world, a fabrication. Because it is a construct, cyberspace is mutable; much of it can be modified and transformed'.[16]

Cyberspace describes the flow of digital data through the network of interconnections: it is at once not 'real', since one could not spatially locate it as a tangible object, and yet 'real' in its effects. Again, cyberspace is the site of Computer Mediated Communication (CMC), in which online relationships and alternative forms of online identity were enacted, raising important questions about the social psychology of the Internet use, the relationship between 'online' and 'offline' forms of life and interaction, and the relationship between the 'real' and the virtual. Cyberspace allows the integration of a number of capabilities such as sensors, signals, connections, transmissions, processors, and controllers sufficient to generate a virtual interactive experience that is accessible regardless of a geographic location.

A forerunner of the modern idea of cyberspace is the Cartesian notion that people might be deceived by an evil demon that feeds them a false reality. This argument is the direct progeny of modern idea of a brain-in-a-vat. Furthermore, visual arts have a tradition, stretching to antiquity, of artifacts meant to fool the eye and be mistaken for reality. This questioning of reality occasionally led some philosophers and especially theologians to distrust art as deceiving people into entering a world which was not real. The artistic challenge was resurrected with increasing ambition as art became more and more realistic with the invention of photography, film, and the present day immersive computer simulations. Now ubiquitous, in current usage, the term cyberspace refers to the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communications take place. There are different culture examples of cyberspace,[17] namely, digimon,[18] ghost in the shell,[19] reboot,[20]tron,[21] virtuosity,[22] simulacron-3,[23] the matrix.[24]

[14] Online systems, for example, create a cyberspace within which people can communicate with one another via e-mail, do research, or simply window shop. Cyberspace can also mean that electrical 'space' or 'a place' where a telephone conversation appears to occur.

[15] Available at <www.wikipedia.org> accessed on March 29, 2014.

[16]S. W. Brenner, 'Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships', *North Carolina Journal of Law & Technology*, vol. 4, no. 1 (Fall), p. 37. Cited in K. Finklea and C. A. Theohary, *Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement* (January 15,2014) p. 6.

[17] Available at <www.wikipedia.org> accessed on June 02, 2014.

[18]Digimon is a set in a variant of the cyberspace concept called the 'Digital World'. The digital world is a parallel universe made up of data from the internet. Similar to the cyberspace, except that people could physically enter this world instead of merely using a computer.

[19] Ghost in the shell is set in the future where cybernation of humanity happens in human space.

[20] Reboot takes place entirely inside cyberspace, which is composed of two worlds; the Net and the Web.

[21] This is a film, where a programmer was physically transferred to the program world, where programs were personalities, resembling the forms of their creators.

[22] This is also a film, where a program encapsulating a super-criminal within a virtual world simulation escapes into the 'real world'.

[23] Simulacron-3 is a novel authored by Daniel F. Galouye which explores multiple levels of 'reality[1] represented by the multiple levels of computer simulation involved.

[24] The idea of 'the matrix[1] in the film, The Matrix, resembles a complex form of cyberspace where people are 'jacked in' from birth and do not know that the reality they experience is virtual

Cyberspace is 'the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries'. In other words, cyberspace is the Virtual environment of information and interactions between people.[25] The United States military has adopted a definition of cyberspace consistent with that laid out in NSPD- 54/HSPD-23. A recently published document of the United States Department of Defence defined cyberspace as a 'global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[26]

Therefore, cyberspace is a superset of the Internet, including also private electronic networks using other protocols. Thus, one of the simplest ways to distinguish cyberspace from the Internet is to say that, all the Internet space constitute the cyberspace but not all the cyberspace constitutes the Internet. For example, apart from virtual space obtainable with the Internet experience, one must not at all times connect to the Internet to operate on a cyberspace. For instance, some programmes, particularly computer games, are designed to create a special cyberspace, one that resembles physical reality in some ways but defies it in others. In its extreme form, called virtual reality, users are presented with visual, auditory, and even tactile feedback that makes cyberspace feel real. Therefore, while cyberspace should not be confused with the Internet, the term is often used to refer to objects and identities that exist largely within the communication network itself, so that a website, for example, might be metaphorically said to 'exist in cyberspace'. According to this interpretation, events taking place on the Internet are not happening in the locations where participants or servers are physically located, but 'in cyberspace'.

3. The Internet and its Viability as a *Locus Criminis*

The Internet is a network of networks comprising of multiple technologies and infrastructures. Viewed as a whole, its basic and unique features[27]which make it a comfortable platform for criminal activities are many. First, the Internet is open. Compared with other forms of mass media, the Internet offers low barriers to its accessibility and was designed to work without the kind of gatekeepers that exist in traditional print or broadcasting media. It is also open because it is inexpensive to obtain the Internet services. What is needed is only a personal computer and a modem, and one can even borrow those items, thereby incurring no cost at all. The Internet is also user-controlled. The Internet allows users to exercise far more choice than even cable television or short wave radio. The user can skip from site to site in ways that are not dictated by the Internet content providers or by the access providers. Users can control what

[25]See the 'National Security Presidential Directive 54/Homeland Security Presidential Directive 23 of United States of America (NSPD-54/HSPD-23)' in *National Security Agency Statement for the Record* by Lieutenant General Keith Alexander, Commander, Joint Functional Component Command for Network Warfare, Before the House Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommittee, May 5, 2009. Cited in K. Finklea and C. A. Theohary, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement*, January 15, 2014.p. 6.

[26] Quoted in K. Finklea and C. A. Theohary, *Cybercrime: Conceptual issues for Congress and U. S. Law Enforcement* (January 15, 2014) p. *6.*

[27] 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) pp. 5 - 6. Available at <www.Cdt.org> accessed on February 22, 2014. Centre for Democracy and Technology is a non-profit public interest organisation working to keep the internet open, innovative, and free. With expertise in law, technology, and policy, Centre for Democracy and Technology seeks practical solutions to enhance free expression and privacy in communications technologies. Centre for Democracy and Technology is dedicated to building consensus among all parties interested in the future of the internet and other new communications media.

content reaches their personal computers and can solely exercise the choice of sites to access. Users can as well encrypt their communications to hide them from government censors and to avoid detection of other criminal activities carried out by them on the Internet.

Another feature of the Internet is that it is global. In the absence of interference, the Internet provides immediate access to information around the world. For a user, it is as easy to send information to, or receive information from someone on another continent as it is to communicate with someone in the same room. With simple e-mail, it is as easy to send a message to another continent as it is to a person next to you. Through the World Wide Web, thousands of newspapers and tens of thousands of other information sources are available from around the world. Researchers recount the benefit of the Internet facility to them as it enables them to access research materials from any part of the world as if these research materials are in the shelves of their personal libraries.

More still, the Internet was designed to be decentralized, to work without gatekeepers, and to accommodate multiple, competitive access points utilised by the Internet users. The absence of gatekeepers of the kind that exist in broadcasting, cable television, or satellite transmission, the availability of numerous hosting sites, and the irrelevance of geographic location mean that material can almost always be published outside the control of governments, monopolies or oligopolies. The effect is that innovators can create a very wide range of applications and offer them without seeking approval of the entities operating the core of the said network. A user of the Internet can have access to any available Internet resources without expressly obtaining the consent of the authors of the said Internet resources.

Further still, the Internet is inexpensive. A computer and an Internet connection are far less expensive than a printing press or a radio station or the kinds of distribution networks that were traditionally required to reach large audiences. In places where the devices that can connect to the network already exist, what one requires to have access to the Internet is only a personal computer system. The Internet is abundant too. The digitization of information and the ability to transmit it over the telephone network, combined with the decentralized nature of the Internet, mean that the Internet has essentially unlimited capacity to hold information. In economic terms, the marginal cost of adding another website, sending another e-mail message, or posting to a newsgroup is essentially zero. But, another technology like that of radio and television is bound by the limited technical capability to exploit the electro-magnetic spectrum. Government regulation of the airwaves was deemed necessary to allocate the scarce resources. The Internet, by contrast, can accommodate an essentially unlimited number of points of entry and an essentially unlimited number of speakers.

The Internet is also interactive as it is designed for bi-directional and multi-directional communications. All the Internet users can be both speakers and listeners at the same time. The Internet allows responsive communication from one person to another, from one person to a group, from a group to one person, and from a group to another. Such is not obtainable in radio and television, except, the people involved appear together in the same radio or television studio or there is an additional facility such as in phoning programme whereby the telephone facility serves as a link between those in the radio or television studio and those outside the studio. Unlike in other communications networks, those interacting on the Internet must not have necessarily established any physical familiarity, although the Internet may give room for physical familiarity through the exchange of videos and photographs. The fact remains that the people interacting on the Internet need not know the identity of each other or one another and must not expressly consent to interact, exchange ideas or Internet resources. Yet, more is that

the Internet makes use of independent infrastructure. The Internet is not linked to any infrastructure other than the telephone system. Dial-up access is available from any telephone that can make an international call. Access to the Internet can also be wireless using modem and satellite based infrastructure, and therefore further moved from effective control of governments.

Finally, even the courts and other institutions have recognized these unique features of the Internet. In a 1996 Communication, the European Commission noted that:

> A unique characteristic of the Internet is that it functions simultaneously as a medium for publishing and for communication. Unlike in the case of traditional media, the Internet supports a variety of communication modes: one-to-one, one-to-many, many-to-many. An Internet user may 'speak' or 'listen' interchangeably. At any given time, a receiver can and does become content provider, of his own accord, or through 're-posting' of content by a third party. The Internet therefore is radically different from traditional broadcasting. It also differs radically from a traditional telecommunication service.[28]

The European Commission Legal Advisory Board, which advises the European Commission on legal matters concerning the European information market, also recognized the uniqueness of the Internet, calling it 'a positive instrument, empowering citizens and educators, lowering the barriers to the creation and distribution of content and offering universal access to ever richer sources of digital information'.[29]The United States Supreme Court, in ruling that the Communications Decency Act of 1996 was unconstitutional and that the Internet merited the strongest protection of free expression, based its judgment on the conclusion that the Internet was 'a unique and wholly new medium of worldwide human communication'.[30] Writing for the Court, Justice Stevens noted that the 'factors that justify censorship of television or radio are not present in cyberspace' including the Internet as a subset of the cyberspace.[31]

4. The Effects of the Nature of the Internet on Investigation and Prosecution of Cybercrimes

The foremost problem in relation to investigation and prosecution of Internet crimes is the inherent shortcoming of national jurisdiction over activities on the Internet**.** A world of difference exists between physical borders and cyberspace. General correspondence between borders drawn in physical space is taken for granted, and which border-lines separating physical spaces are of primary importance in determining legal rights and liabilities. Under the law, it is not disputed that geographical boundaries make considerable sense in the real world for their relationship in the development and enforcement of legal rules. The Internet, on the other hand, undermines the relationship between online phenomenon and physical location in relation to the power of municipal governments to assert control over behaviour on the Internet,

[28]Commission of the European Communities, Communication from the Commission to the Council, *et al.,* 'Illegal and Harmfijl Content on the Internet', COM (96) 487 Final, October 16, 1996, available at <http://www.drugtext.org/library/legal/eu/eucnetl.htm> accessed on March 23,2014.

[29] Available at <http://www.drugtext.org/libi-ary/legal/en/eucnetl.htm> accessed on March 23, 2013.

[30]*Reno v American Civil Liberties Union (supra),* footnote 42 of chapter one of this research work, p. 19. The Supreme Court decision is available at<htt://www.law.coniell.edu/supct/html/96-511.ZS.html>, accessed on February 2, 2014.

[31] Justice Stevens, however, used cyberspace interchangeably for the word, internet. See Chapter Three (2. 3. 3) of these research work for the distinction between the internet and cyberspace.

the effect of online behavior on individuals or things, the legitimacy of a local sovereign to regulate a global phenomenon, and the ability of country's government to give adequate notice of which sets of rules apply.[32]

The structure of the Internet diminishes the chances for enforcement of laws and regulations that are national in scope. Attempts to impose national barriers against subversive or culturally polluting information are readily circumvented. National speech restrictions, for instance, can only be enforced directly within the territory to which they apply. The Internet is global and so is the flow of information. Hence, people who disseminate information that is illegal through the Internet in one country can easily transfer their operations to another country without similar prohibitions, and effectively reorganize their circulating action within a very short time. For the recipients of such information, redeployment is hardly noticeable in an environment dominated by the World Wide Web where information is accessed and retrieved by simply clicking on the relevant information links. Since distance from one location of information resources on the Internet is irrelevant to the recipient, access to the relocated information is easy and straightforward.

Nevertheless, the Internet is not absolutely a free speech domain but may be subject to some national restrictions, even though the ability to enforce activities taking place on the Internet has the most tenuous connection with physical boundaries. In an attempt to enforce the activities on the Internet especially as it concerns what citizens may access on the Internet, some national governments have maintained that they have the right to regulate the activities of companies or individuals 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'.[33] However, the Florida Attorney General, while making a statement to like effect conceded that the Attorney General's office' should not waste time trying to enforce the unenforceable'.[34] This issue can simply be framed in this manner: Can a person who sends data through the Internet properly be forced to follow the laws or defend himself in court in any forum in which the data can be accessed on the Internet?

In the United States of America, the courts have approached this question by following the concept of personal jurisdiction, keeping in mind the complication caused by the offender being a citizen of another sovereign nation.[35] In the case of *Playboy Enterprises Inc v Chukleburry*,[36]the defendant, a resident of Italy had established a website on a server in Italy bearing the name, 'Playmen', featuring sexually explicit photographs of women. Fifteen years earlier, the same court had issued a permanent injunction against the defendant from using the same name, 'Playmen' in the title or subtitle of magazine published, distributed or sold in the United States of America. The defendant argued that although the site could be accessed from the Internet in the United States of America, he was not actively selling or distributing his products in United States because users had to 'come to Italy' to access the photos. Thus, he argued that his act of posting images on a server in Italy could not be viewed as selling or

[32]See K. Nandan, *Law Relating to Computers Internet and E-Commerce* (5th edn, India, Universal Law Publishing Co. Pvt. Ltd, New Delhi, 2014) p. 275.
[33]*Ibid.*
[34]*Ibid.*
[35]*Ibid, p. 276.*
[36]939F. Supp. 1032.

distributing those images in the United States of America. The court ruled that customers had to register with him and receive a password, and so the defendant had reason to know that some users were located in the United States of America. The court admitted that it did not have the power to order the defendant to close down his site because both the defendant and the server are located in Italy and stated that any attempt to do so merely because the site is illegal in the United States of America would be 'tantamount to a declaration that this court and every other court throughout the world, may assert jurisdiction over all information providers on the global world wide web'. But the court ordered that the defendant must refrain from accepting customers from the United States of America.

According to Nandan,[37] the above ruling represents a tremendous and quite dubious assertion of authority by the court. The holdings present two difficult questions. Firstly, how does the court intend to enforce its orders if the defendant fails to abide by the orders? Secondly, is it possible for the court to expect a United States' content provider who transmits data that are legal under United States law to comply with a similarly intrusive ruling from a court in Rome or elsewhere? Hence, it is clear from the above that the court's ruling illustrates the complex problem presented by the Internet and particularly exposes the inherent shortcoming of national enforcement in the Internet related matters.

Another major obstacle to investigation and prosecution of suspected Internet criminals is in relation to evidentiary regime and the fate of Internet materials. Hence, how can one apply the law of evidence to materials obtained from the Internet bearing in mind that evidence is regulated by the body of law relating to the admissibility of what is offered as proof in a legal proceeding. Evidence is the collective mass of things presented before a tribunal in a given dispute. It includes testimonies, documents and tangible objects that tend to prove or disprove the existence of an alleged fact.[38] Although modernity is fast embracing mobile technology such as mobile phones, almost all evidence to prove facts in litigation involving the Internet are computer generated. Either way, the crux of the matter is that the evidence is processed through a mechanical device.[39] In Nigeria, the contents of documents obtained from computer or other electronic or mechanical process are now admissible as primary evidence. Section 86 (4) of the Nigerian Evidence Act[40] provides that, 'Where a number of documents have all been made by one uniform process, as in the case of printing, lithography, photography, computer or other electronic or mechanical process, each shall be primary evidence of the contents of the rest....'[41] . It also provides that 'in any proceeding, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible....'.[42]

However, until 2011, the Nigerian Evidence Act which was enacted in 1943 was procedurally inadequate to cover the present advancement in technology with the concomitant sophistication employed in the commission of economic and financial crimes to the extent of not allowing computer generated evidence in court. In *Yesufu v ACB*,[43] the question as to whether 'entries in books of account' as contemplated by the then Evidence Act included computer generated

[37]K. Nandan, *Law Relating to Computers Internet and E-Commerce*, p. 276.
[38] See B. A. Garner *et al* (eds), *Black's Law Dictionary*, (9[th]edn, United States of America: West Publishing Co., 2009) p. 635.
[39] See K. Nandan, *Law Relating to Computers Internet and E-Commerce*, p. 51.
[40]Evidence Act, 2011.
[41] See also, section 63 (2) of the Indian Evidence Act, 1872.
[42]Section 84, Nigerian Evidence Act, 2011.
[43](1976)48. C. I.

statements or printouts became an issue of debate. The Supreme Court of Nigeria only expressed by way of *obiter* a willingness to interpret the section more liberally in view of contemporary business practice and methods when it noted, *inter alia,* that:

> the law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of computers. In modern times reproductions or inscriptions or ledgers or other documents by mechanical process are common place and s. 37cannot therefore only apply to books of account so bound and the pages not easily replaced.[44]

Computer generated documentary evidence can be classified into three. The first one encompasses calculations or analyses that are generated by the computer itself through the running of software and the receipt of information from other devices such as built-in clocks and remote sensors.[45] In the second classification are documents and records produced by the computer that are copies of information supplied to the computer by human beings.[46]The third category contains information that combines calculations or analyses that are generated by the computer with the information supplied to the computer by human beings to form a composite record.[47] According to Nandan,[48] these three types of computer generated documentary evidence are respectively termed as real evidence,[49] hearsay evidence[50] and derived evidence.[51] The admissibility of computer generated documentary evidence has certain conditions attached to it and those conditions vary among different jurisdictions. Perhaps, the reason for imposing such conditions for the admissibility of computer generated documentary evidence is because it is less trusted since it is very susceptible to manipulations, and so requires a certificate as to the authenticity of the evidence.

In India, the Companies Act requires the media on which the data is stored to be 'scanned' and 'authenticated' by the Registrar.[52] In the United Kingdom, under Civil Evidence Act 1968 and section 69 of the United Kingdom Police and Criminal Evidence Act 1984, computer evidence is only admissible if it satisfies two tests. The first is that there must be no reasonable ground for believing that the statement is inaccurate because of improper use of the computer.[53]The second is that the computer must have been operating properly at all material times or at least the part that was not operating properly must not have affected the production of the document or the accuracy of the contents.[54] In *R.v Shephard,*[55]the accused, Mrs. Shephard, was alleged to have shoplifted from Marks and Spenser store in London. She contended that she had thrown

[44] See generally L. Ani, 'Cyber Crime and National Security: The Role of the Penal and Procedural Law', in *Law and Security in Nigeria,* pp. 197 - 232, available at <nials-nigeria.org/pub/lauraani.pdi> accessed on October 17, 2014.
[45]K. Nandan, *Law Relating to Computers Internet and E-Commerce,* p. 53.
[46]*Ibid.*
[47]*Ibid.*
[48]*Ibid.*
[49] For instance, if a bank computer automatically calculated the bank charges due from a customer based upon its tariff, the transaction on the account and the daily cleared credit balance, that calculation would be a piece of real evidence.
[50] For example, cheques drawn and paying-in slips credited to a bank account are hearsay evidence.
[51] For instance, the figure in the daily balance column of a bank statement which is derived from automatically generated bank charges (real evidence) and the individual's issued cheques and paid-in entries (hearsay evidence).
[52]Section 610A of Indian Companies Act 1956.
[53]Section 69 (1) (a) of United Kingdom Police and Criminal Evidence Act 1984.
[54]*Ibid.* Section 69 (1)(a).
[55](1993)1 All ER 225.

her receipt away. The Prosecution relied upon the store's central computer system's records. Every item in Marks and Spencer store has a Unique Product Code. So, a store detective was able to ascertain whether the items in question had been sold by examining all the codes on a till roll on the day in question. The store's central computer issued the date on each till roll. Thus, the question before the House of Lords was whether this evidence should satisfy the requirements of section 69 of the 1984 Act. Lord Griffiths made the following statement: 'If the prosecution wishes to rely upon a document produced by a computer, it must comply with section 69 in all cases'.[56]

In the same vein, section 84 (2) (c) of the Nigerian Evidence Act 2011 provides its own condition, namely, that throughout the material part of the period over which the computer was used, the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents. To ensure authenticity of the document, section 84(4)(b)(i) of the Nigerian Evidence Act provides thus:

> In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate - (a) identifying the document containing the statement and describing the manner in which it was produced; (b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer, (i) dealing with any matters to which the conditions mentioned in subsection (2) above relate; and purporting to be signed by a person occupying a reasonable position in relation to the operation of the relevant device or the management of the relevant activities, as the case may be, shall be evidence of the matter stated in the certificate; and for the purpose of this section it shall be sufficient for a matter to be stated to the best of knowledge and belief of the person stating it.

These respective sections 69 of United Kingdom Police and Criminal Evidence Act 1984 and section 84(2)(c), (4)(b)(i) of Nigerian Evidence Act 2011 pose a requirement such that unless the evidence sought to be adduced meets the criteria, it is inadmissible. Other conditions required to be satisfied under the Nigerian Evidence Act include:[57] (a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, or by any individual;(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;(c) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

The foregoing conditions are powerful tools to ensure that both prosecution and defence rely only on appropriate and reliable evidence. The certification envisaged in the above sections is

[56]K.Nandan, *Law Relating to Computers, Internet and E-Commerce*, p. 57.
[57]See section 84 (2) (a) (b) (d) of the Nigerian Evidence Act 2011.

either oral evidence to tender a written certificate by a person occupying a responsible position in relation to the operation of the computer[58] or oral evidence on the reliability of computer evidence which can be challenged in cross-examination. One of the problems associated with this certification of the Internet evidence is the difficulty of proving the continuity of the Internet evidence, especially when considering the fact that messages over the Internet split into 'data packets' and travel individually through different routes from computer at origin to computer at destination. In demonstrative terms, an e-mail does not serially go from Y to Z, but in a number of parts, which reconstruct themselves at their destination (Z). The number of computers this e-mail passes through in its journey could be from ten to thousand[59] or even million. For example, in relation to hacking, it would be expected that the prosecution should trace a line of access from the hacker's own computer to that of the victim. Only the simplest Internet hacking cases will feature two computers and an identifiable user. More regularly, a hacker's command will pass through many different computers across the Internet and those computers that act as couriers could be located anywhere in the globe. Moreover, it is well known that hackers rarely attempt to gain access to their victim's computer directly. Their preferred method is to log in to one computer on the Internet and from there log in to another computer. Thus, any discontinuity in providing adequate proof from first to the final unauthorized access may raise the court's reasonable doubt that the accused was not the actual person responsible for the final unauthorized access.

Another problem associated with certification is observed in relation to spoofing. Spoofing involves using a false identification to gain access into a computer. A hacker is able to do this by having previously obtained actual passwords, or having created a new identity by fooling the computer into thinking that he is the system's operator.[60] Here, the prosecution must establish that the hacker at his own computer was the person who has logged into other countless computers and what that means is that the prosecution will be required to obtain multiple certificates representing the actions of the hacker in each of those computers. Each certificate must adequately verify the workings of each of the computers in that continuity chain. This is to ascertain the actual identity of the hacker and whether there was any trace of malfunctioning[61] of the computers. Since the hacker may attempt to tamper with the logging software actually used by the system, it poses a problem of admitting that the log has been tampered with at all, which would raise suspicion that the computer was not operating properly at that material time. If the prosecution is subjected to this kind of rigorous procedure for tendering electronic evidence, then there is no doubt that such evidentiary regime poses serious problem to the successful prosecution of the Internet-based cybercrimes. It is herein argued that if the aim of the evidentiary regime is to facilitate the spread of the Internet usage and allied technologies as well as to ensure more success in enforcement of cybercrimes, the above requirement will hamper the efforts.

However, the need for having a check on computer generated evidence cannot be over-emphasized. This need is due to the fact that computers arc machines, unreliable and unavailable for cross-examination in court. Thus, till now, the burden of satisfying the computer operational requirement rested on the proponent of such evidence. The law imposes almost an impossible requirement on the proponent. Apart from the problem of obtaining the

[58]Para. 8 (d), Schedule 3 of United Kingdom Police and Criminal Evidence Act 1984.
[59]K. Nandan, *Law Relating to Computers, Internet and E-Commerce,* p. 59.
[60]*Ibid.*
[61]*In DPP v Mckeown* [1997] \ W. L. R. 295, Lord Hoffman in his opinion for the unanimous House of Lords, held that, 'A malfunction is relevant if it affects the way in which the computer processes store or retrieve the information used to generate the statement tendered in evidence'.

certificates, the more number of computers required to be certified increases the possibility of one of them not working reliably, thereby disqualifying the evidence. The Internet imposes an irreconcilable problem with such requirement since every message travels through numerous and different computers.[62] The burden of proving the malfunctioning of the computer should lie with the defence. The malfunction must be such that it is affecting the data sought to be adduced and if there are other malfunctions which do not affect the reliability of the evidence, they should not be reckoned with. In this regard, in order to ensure a balanced approach whereby computer-generated records are not abused because of the strong evidential presumption, it could be laid down that if the defence proves the existence of a malfunction in the computer in question, it should be up to the prosecution to prove that such malfunction did not affect the data sought to be adduced.[63]

The above approach envisages a reversing of the presumption contingent on a demonstrated objection by the defence. This would balance out the problems with computer generated evidence as regards the Internet and would ensure that the evidence adduced is reliable and not prejudicial to either party. This would impose a reasonable and balanced check on the admissibility of the Internet and computer evidence. However, this framework does not envisage the unfettered admission of the Internet based computer generated evidence. It rather provides the criteria for the recognition of electronic record as not being valid solely on the ground of it being in an electronic format.[64] This framework provides a method of adducing and objecting to electronic records on substantially cogent grounds, and not merely because of the format of the record or the immediate need to use the record in arresting a particular evil. In any event, the framework does not provide any unnecessary burden on either party, but only meant to ensure that the evidence sought to be adduced is reliable and authentic. The discretion as to the proof of objections should rest with the courts. The courts should be given discretion as to whether the objections relating to malfunctions and relevancy thereof, imposed on opponent and proponent, respectively, should be proved by oral, documentary, real, demonstrative or any other kind of evidence. This discretion should be given because any hard and fast rule regarding proving of objections in the context of advancing technology of the Internet would not be technology neutral and would prejudice the legal rights flowing out of this technology. In the case of G. v *DPP*,[65]the court held that it has the discretion and entitlement to admit expert testimony as to whether video testimony should be admitted.

More still, the next issue that needs to be considered is the application of 'Postal Rule' in relation to electronic records. With the emergence of the Internet, a pertinent question arises as to whether in the case of communication of electronic messages, the general rule or the exception with rule adopted in case of postal correspondence will apply. The Indian Information Technology Act[66] has a copious provision in this area of law. In the first place, the Act provides that an electronic record shall be attributed to the originator[67] 'if it was sent by the originator himself; by a person who had the authority to act on behalf of the originator in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically'.

[62]K. Nandan, *Law Relating to Computers, Internet and E-Commerce,* p. 61.
[63]*Ibid.*
[64]*Ibid.*
[65](1997) 2 All ER 755.
[66]Information Technology Act 2000 (as amended in 2008).
[67]*Ibid*, section 11.

Section 13(1) of the above Act provides that the dispatch of an electronic record occurs when it enters a computer resource[68] outside the control of the originator. This provision that the computer resource to which the message is sent should not be under the control of the originator is well made out, as it will avoid a situation whereby the originator would get back to the sent message to manipulate same on selfish ground. The time of receipt of an electronic record shall be determined as follows:[69]

> a. If the addressee has designated a computer resource for the purpose of receiving electronic record, (i) receipt occurs at the time when the electronic record enters the designated computer resource; or (ii) if the electronic resource is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is received by the addressee.
> b. If the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

The addressee of any electronic record is expected to acknowledge receipt of same upon the receipt of the said electronic mail by him. When the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such an electronic record by him, then unless an acknowledgement has been so received, the electronic record shall be deemed to have been never sent by the originator.[70] Where the originator has not stipulated that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by[71] (a) any communication by the addressee automated or otherwise; or (b) any conduct of the addressee sufficient to indicate to the originator that the electronic record has been received. This means that the acknowledgement of receipt of an electronic record can, instead of the addressee using the same electronic means, be by means of putting a phone call across to the originator, or by sending a messenger to inform the originator, or by even sending the acknowledgement through postal agency. It is important to point out that any means which the addressee decides to adopt must meet up with the stipulated time, if any. It is always faster to use the same electronic means, especially when time is of essence.

Where the originator has not stipulated that the electronic record shall be binding only on receipt of acknowledgement and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him, and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.[72]

---

[68] Section 2 of Indian Information Technology Act 2000 provides that computer resource means computer, computer system, computer network, data, computer data base or software.
[69] *Ibid*, section 13(2).
[70] *Ibid*, section 12(2).
[71] *Ibid*, section 12(1).
[72] *Ibid*, section 12(3)

5. Conclusion

This paper has studied the features of Internet regime and discovered its utter facility for cyber criminality. Yet most Internet criminals get away with it due to structural and technical difficulties associated with investigation and prosecution of offenders. This situation no doubt impacts and threatens nearly every transaction over the Internet. Most Internet crimes take place across international borders, while law enforcement agencies are always limited to jurisdictional boundaries. Sometimes, law enforcement agencies of one nation would work with another nation's law enforcement organs, but these occasions are rare and sometimes unsuccessful due to possible non-co-operation. It is revealed that another huge impediment to successful prosecution and conviction is the lack of official, legal evidence. Most courts accept 'the best representation' of evidence recorded during the commission of a crime. But most computer systems and many networks do not collect any evidence at all, much less evidence that might stand a chance of holding up in court. Again, few victims or victim advocacy groups have the resources, technology, or funding to pursue Internet criminals. Unfortunately, the amount lost usually pales compared to the cost of the resources that would be needed to recover the funds. In the light of the above issues and more, an urgent demand is placed before modern technology to evolve adequate techniques of identification of Internet users as an antidote to the prevalent anonymity on the net. There is also a dire need for legislatures to pursue progress in science and technology and not make laws that lag behind same.