Journal of Theoretical and Applied Information Technology
31st August 2013. Vol. 54 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REGULATION ON ACCESS TO INTERNET: PROBLEMS AND SOLUTIONS

MUTUA NICHOLAS MUTHAMA
University of Sunderland
nicholas.mutua@sunderland.ac.uk

ABSTRACT

Regulation on access to Internet is a tool that is crucial to the growth of any nation. Some problems arise as attempts to implement regulation on access to Internet are concerned in both developing and developed countries. For example, privacy and lack of it on online information is a subject that has challenged the existing legal and regulatory infrastructure of access to Internet. Other problems to Internet access pointed out in this paper include; inadequate Internet regulations, inappropriate legislation, security, piracy, hacking online transaction, cyber crime, unsolicited e-mail, racism and xenophobia.

To overcome these problems, some remedies are necessary. Regulation for user and internet service providers, provision of security of systems, Education, content restrictions on unsolicited mails, continued assessment of the internet and protection against access to illegal information is solutions suggested. The paper concludes by looking at how academic institutions, work places, business atmospheres have access to Internet and the need to strengthen the current legislation and enforce procedures not only to system administrators but also to employees. Finally a recommendation of computer policy in organizations is made towards achieving a controlled access to the Internet.

Keywords: *Internet Regulatoins, Inadequate Internet Regulations, Inappropriate Legislation, Security, Piracy, Hacking Online Transaction, Cyber Crime, Unsolicited E-Mail, Racism And Xenophobia,*

1. INTRODUCTION

Today, Internet has reduced the world to a global village where people share information. Barlow (1992) asserts that the rate at which Internet is growing per month will put human beings online worldwide in few years to come. As such academic research, online transaction, communication has also increased. Countries (both developed and developing) are venturing into this technology with no prior knowledge of the consequences and the legal operation framework. Johnson (2000) suggests that there should be a continued assessment of the Internet, which is the backbone of the information society. This assessment should focus on societal worth and be based on the following questions.

a) How is the Internet governed or should it be?

b) How is autonomy of nations (states or local communities) recognized in policy decisions regarding the Internet?

c) Are the economic interests shaping the Internet allowed to undermine its potential to serve political and public interests or should it be?

d) Is freedom of expression protected?

e) To what extend is there privacy on the Internet and to what extent is the medium a medium of surveillance (Johnson, 2000)

For instance, the Y2K phenomenon is an example of problems caused by accurate prediction. It was expected that computers would not input some figures such as zero during the year 2000 but this was not the case. This is a problem caused by continued use of the Internet and led users to have a more limited role in their thinking.

Hornes (2003), asserts that we can use our knowledge of the past (and we surely can talk about our knowledge of the past) as a guide to action. This does not necessarily imply that the future will be like the past.

Internet has been used by spammers worldly to send Spam with or no knowledge of users. Although different nations posses different protection laws, their generality in character may not be applicable in fighting cyber vices. Palfrey (2005) notes that different states use different laws to fight such acts as piracy, Spam and security whose originality is cyber related. However, the laws do not yield the required results. As a result therefore, training of professionals of computer and Internet users is necessary. It will promote the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ethnical and legal protection of information, security, privacy, online transactions, workplace, and business atmosphere and information and communication technologies. The various problems facing the Internet and their related remedies are outlined.

2. Problems

2.1 Hacking

Over the last two decades, there has been advancement in new technology discoveries. Certain technologies however good they are can be destructive. An example is the use of technical know-how by hackers to make money by intruding, changing or interfering with networks. Such acts as a banking fraudulent deal affects the banking sector adversely. Development of new technologies and their applications has lead to problems facing the Internet access and use (Blowback, 2004). This calls for proper planning before applying new knowledge in the world. The principles of new technologies are widely used by hackers. In institutions of higher learning or firms, hackers may be consultants or system administrators. Due to their roles, it is not easy to detect the crimes and if it happens, is after a spell of time. This is due to the trust build on the consultant who may have bad intentions in his operations.

(Capron 1996) asserts that the discovery of many computer evils is intentional. Richard (2005) provides a case on communications Act. In America, hopes of spreading phone lines at low rates in was provided in 1934 communications Act, phone companies were required to subsidize rates in low income areas by increasing rates in wealthier areas. This agreement, which provided telephones into the homes of many who otherwise could not have afforded it, was sold to the providers with concessions, such as non-enforcement of some anti-monopoly laws. Like the phone system, Internet Acts do exists, that provide regulations on hacking.

Technological advancement has resulted to spamming. The emergence of cheap electronic services and communication via mobile phone has led to increased spamming. Richard (2005) explains that security threats' including viruses are due to the conveyance of Spam brought about by digital communication dependency. (Ngugi 2005) says that lawyers have put forward that information age has brought many gains that are imperfect. Thus it is a clear indication of how the applications of new technologies such as Internet have adversely affected the economies of developing countries.

Expansion of Internet communication has led to emergency of more pronounced and complicated computer crimes such as hacking for the police to handle (Wikipedia, the free encyclopedia 2006). The threat is technology based whose associativity is based on poor police officer training. The police officers in most cases lack technology based training and so unable to carry out investigations that go hand in hand with the current technology. Capron (1996) observes that if law enforcement's agents detect a hacker, they do not fully understand the complications associated with such computer related fraud. In situations of no comprehension, they are unable to enforce law.

2.2 Privacy

One of the problems posed by use of Internet is the so-called privacy. This is when one is required to obtain permission from the website so as to use or analyze the data. Among the questions put into consideration has to do with personal privacy and the use of certain kinds of Internet search facilities to stake in individuals in cyberspace (Frances 2002). Certain countries have put in place the control measures over the access of information from the Internet. But the main issue is that it is possible to regulate such access without getting into conflict with the values that justifies the freedom of global access to the Internet. The cyber society is of great importance in this situation and so the question of whether it is right to deny access to the Internet services has to be put into consideration. A quote from Richard G Platt, that "Privacy or lack of it is a subject that can inflame hearts of most people. Many of the potential abuses of privacy online have analogs in the "mundane" world. But the new technologies, along with a perceived impersonality, make the infractions on line harder to pin down (Neumann 1991). With the large increases in the number of non-technical users come greater risks of both victimization and inadvertent abuse.

Countries such as Singapore have put in place measures such as proxy servers in a bid to limit access to site that hold information that is cultural integrity and political importance (Singapore 1996 Press release). The main aim in this scenario being to offer privacy to matters that are considered to be of national importance. If access

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is allowed then it is determined whether it is free or at a fee. Richard (2005) notes that there will most likely be free public access to public documents, such as governmental records and discussion groups and that are nothing to pay. However, the problem arises when there is some data owned by individuals that may be of great value to the public at large. In creating this data, costs might have been incurred. It might be necessary to subsidize partially for the cost of information. That is why to access information over some websites one may be required to subscribe and even purchase some of the articles. A case illustration of this is the Athens account. In this, so access data one has to subscribe to become an authenticated user. One who is not authenticated to access data from the emerald group publications cannot be allowed to do so. By so doing, personal information has to be protected.

2.3 Piracy

The emergency of Internet use as a means of communication in workplaces, businesses acts on entry points to software piracy. Transactions that are not legal are carried via the network being unnoticed. For instance, trans-border, gambling can take place throughout the network with no knowledge of those at management level.

For any business venture to succeed, ethical and legal practices should be put in place. For purposes of business survival, software piracy is a practice if supported by management can be carried out by employees in small firms effectively (Boulton ud). The problem is piracy with the work place/business ventures where the top management may o regulate their users. If this happens then guidelines on ethical practices in these sectors are violated. Experts, who possess technical know how mostly, practice data piracy. IT managers complete some projects using pirated software certain projects with an aim to earn money. In developing countries, this problem of piracy is more pronounced since people have to earn a living by using illegal business practices.

Inadequacy in policy guidelines is one of the causes of unethical computer uses in different economic sectors. One of the ways of promoting piracy is invading a workmate when using a computer. Weckert (2000) notes that restricting Internet use in the workplaces has its implications. When one pirates software, the existing copyright laws are violated. Erick (2006) explains that it is illegal for unauthorized use and distribution of software copies in absence of authority. Software development and property ownership laws are quite different. One cannot use physical object without the consent of the owner. But with software, it is different – this is why piracy is deep rooted in developing countries.

There are many legal cases that exist concerning whether copyright and patent rights are applicable to computer related software. This includes Whelan Associates (1990). In all the case the court ruling was that software protection was guaranteed. As the new technology emerges, Erick notes that Internet can distribute original software. Thus, regulation or legislation cannot easily changes software piracy attitudes (Wests 1995). Music piracy, phonographic piracy problems are not simply legal problems, and cannot simply be solved by legal means. In Kenya, the penalty of software piracy is fifty thousands or an imprisonment. Yet this is not the solution since the vice still goes on. In Kenyan legislation, issues of rights to intellectual property are not taken into consideration. These problems add weight to Koigis (2006) scenario that explains a man inventing a condom dispenser but little was reaped from it. Piracy by an NGO was detected but on seeking a legal redress it was fruitless.

2.4 Security of Networks

Data creators and holders as much as they try to maximize privacy, problems still arise. For the last few years, the security of network has not been given the attention it deserves. Richard (2006) argues that when a hacker gets in, the only thing protecting the network is the hacker's good intentions. It is in rare cases when such circumstances exist. If under any circumstance information that was deemed confidential is made public then it will be argued that system administrators might have failed to secure his/her network neglecting the ethical obligation of protecting the privacy of the owners of that information. Lack of security to networks may result to scramble of information and then this can be intercepted by a third party and read. Crocker (1994) suggests of a method called sniffing, currently used in holding valid passwords. Network administrators have the responsibility to maintain all the passwords and keep them secret. David (1999) notes that success of the Internet and security problems it faces are greatly contributed by the openness of the environment. The security frameworks implemented in the networks environment and the current developments and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

future trends involving the Internet. Security laps is one of the ways the Internet could potentially affect critical information should possess guaranteed security.

2.5 Electronic Banking

The growth of Internet as a new technology has attracted many people to transact online. A technology that is new in the market faces challenges as much as it enjoys benefits. That's why, this new technology has the threat of some people being able to hijack dealings with ease inform of email messages .The popularity of e-banking can be traced back to the last few years. As Internet transactions intensify, chances of coming mistakes also broaden. Banks have started marketing themselves over the Internet, e.g. HFCK, Barclays Bank etc. As this is an added access to most people, it poses some threat from the access. The great of all is the threat of some of these banking institutions may not be legitimate, Daphyne (1998). For instance, in Kenya the co-operative Union Bank collapsed and so many people lost a lot of money.

This means that on-line banking encourages/attracts many people because it may be time saving. Due to professional looking for marketing or public relations firms, e banking has increased tremendous. This is a trend as reported by Daily Nation (2008), that Google came from nowhere and is now ranked as the 20th most valuable company in the world according to inter-brands 2007 Global bank valuation.

In Kenya, the Nairobi Stock Exchange has switched to Wide Area Network that allows trading away from offices. This was a move towards achieving remote trading where dealers will operate from their places of work. Though, the cost of implementation was high (Ksh 35 million), the WAN was a follow up of the Automated Trading System (ATs), commissioned in September 2007. ATs allowed brokers to post buy and sell orders and have them matched automatically making a change from the open out cry system.

"Information technology has been a key driver in business and the Stock Exchange is not exempt," says Mr. Bitengo. Satchu (2008) notes that Kenyans need to understand that info-mediary services (for which they will pay a small amount) can have very positive and magnified effects on their personal balance sheets.

3. SOLUTIONS TO THE PROBLEMS

3.1. Regulations on Internet users and Internet Service Providers.

Internet has reduced the modern world into a global village, where the barriers of time and distance are disappearing (Barbara 1999). The access to Internet is one of the elements to be put into consideration for most sectors of economy in developing countries greatly rely on this new technology. Countries need to impose mechanism of self-regulation. Illegal business transactions or illegal information access should be prohibited from users by internet service providers by establishing codes of conduct, palfrey notes, similarly, combined efforts of internet service providers and law enforcement agencies can control the problem of spamming. ISPs are close to the source of spamming and so in conjunction with regulators can succeed in curbing the vice, Palfrey (2005). Unethical practices towards Internet access can best be solved through regulation. The question arises whether it is ethical to deny access to information that is deemed of great importance to the public. Is it possible to control the access to the Internet without raising conflicting issues to the cyber society? Clearly, information is power and attempts to deny the society this power may be against human right to access to information.

In developed countries, for instance USA, laws in books about Internet users contend physical world rules do not apply in cyber space. Those rights apply to tangible assets should also be applied to electronic form. The laws and court decisions have not defined incidences such as Internet intrusion, vandalism and theft. As the technology grows rapidly, there is a need to develop laws and regulations to address the problems facing this sector. Internet as a means of communication, it has been used to send messages through emails. Email messages meant to be private become public due to the to lack of ethics or laws.

Laws have been developed/passed over the past decade in USA over the Internet use. Privacy, computer security and the Internet laws have been passed. Mainly the laws address access to data remotely and computing since it poses great threat not only to business but also to the public. They include:

a) The computer Fraud Act. Daphyne (1978) notes that the law was to curb connection to any federal computer whose

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

intention was defraud. Protection level in this case depends on the organization.

b) **Electronic communications Privacy Act** (ECPA) passed in 1986, to ensure privacy of e-mail. It denies one the chance of using, disclosure of messages or hijacking emails without the owners' permission. The motive was to protect private messages from being accessed by government or individuals with no legal authority.

c) **Private laws** – in California, a proposed state privacy act was set up to provide privacy of computers. Daphyne (1998) notes that computer crime victims are all liable to this protection.

d) **Telecommunication Act**

It regulates content and nature of the information placed in the Internet and conveyed through the same. Its main aim was to minimize the online and Internet consequences in service delivery.

3.2. Copyright Protection

The information contained on the Internet can be accessed, pointed, downloaded and send to other people. Many are times people copy information found on the Internet. What are the ethical or legal implications of this? The problem arises when one argues that the information found online is not an asset (tangible) and so one cannot claim its ownership. Thus the protection of intellectual property is possible with the existing laws. Ownership over the intellectual property is referred to as copyright. Most documents found on the Internet had the label of copyright from the owner.

In the USA copyright laws have been put in place. Ackermann (1995), states that USA has put in place copyright laws, the Universal Copyright Convention or the Berne Union information found on the internet with no fear associated to it can be used for free. Most of the articles found on journals require one to subscribe so as to purchase at a given fee. Through this one able to access material and again copyright are also preserved. It is required that one puts information on the Internet expecting a credit. Copying somebody else works denies the person the credibility he/she deserved. But the question arises that what is type of the information to be put in the Internet? According to Ackermann, when information is in "fixed form", then US copyright laws starts applying. Copyright laws need to be put in place in curb plagiarism, which is a rampant vice in academics. In developing countries, it is more pronounced, with a lot research both at undergraduate and postgraduate being reduced to little substance. The introduction of JISC, by the University of Sunderland is a move towards eliminating this problem.

3.3 Policing Internet Privacy

Lucas (2004) asserts that privacy is a relative concept. Total privacy may not be achieved but attempts to minimize privacy intrusion have been tried. It is a matter of suitability for the matter at hand. Privacy plays a fundamental role in shaping of everyday social relationships and so if denied, and then the social and ethical rights of a person are also denied. The right to private doesn't negate the importance of accountability and transparency. It is the responsibility of an individual to control who has access to his online services, who knows what about him. Electronic access is becoming more and more immediate and direct. It is the articulation of a new set of protocols that will enable us to cope with the demand of privacy (Lucas, 2004).

The problem of piracy caused by access to the Internet can be best solved through counseling through the Internet. Dave (1999) describes privacy as an important part of the encounter that is a level of intimacy that of parent or child or husband and wife. Most of times people will be interested at knowing secrets of a certain client is sharing with him. This will eliminate the problem of financial exploitation since one can be counseled on how to go about private discussions in chat rooms and even to avoid exchange of credit card numbers that may lead to loss of money. If the communication was insecure (no privacy), then the client is bound to miss the chances of getting the dangers. Internet being a sophisticated technology, policing the problems of privacy may be difficult. One of the ways to harm Internet user against privacy intrusion is reliance over the past. Experience is the best teacher, and so in cyberspace, it is crucial to put cases that have happened on board so that people can be aware of the dangers a head of privacy in Internet use. Aitkan (1995) observes that the availability of Internet to the public is attributed to its growth. Since the last decade, an estimate of between 5-8 million people per day access the network.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.4. Address to theft of data and piracy challenges.

The distribution of software is a threat to the Internet that is rampantly growing. Nowadays, with the emergence of new technology, duplicated application can easily be passed over to the Net. Daphyne refers this illegal act of software distribution as piracy. Legislation or regulation will not easily change software piracy attitudes.

Piracy of software can best be solved by appealing to moral standards and reasoning. At organizational level, policies and regulations on ethical software use are influenced by moral standards whilst at individual level, moral reasoning influence the legislation.

Richard (1995) describes a highly effective hardware (clip) based encryption technique, called "clipper" as a solution to threat to the privacy of unprotected data out on the net. In this method, the data can be scrambled with such effect as for ender the message nonsense to almost anyone, except the government itself. The keys to the code would be kept by two separate agencies and presented in case of a court order is issued.

3.5 Education

With the increased use of the Internet, users need to be fully trained on the threats it faces as a technology. Richard (1995), believes that time has arrived where people must reduce the power of knowledge. Superpowers, like America are investing a lot of money in the IT sector and so any challenges facing the sector need to be addressed adequately. Learning in cyberspace has greatly increased as technology change. For technology or informationally illiterate society, job prospects are rendered fruitless. In Kenya for example, introduction to free Primary Education has seen the drop in level of illiteracy. If the government introduces computer classes and further e learning, then this will be a way out to some of the problems befalling this means of communication.

Governments in developing countries should introduce youth training centers to the youth who are prone to Internet access and use. By doing so, the youth who are data pirators or even music, would understand the adverse effects of piracy. Organizations and learning institutions, such as colleges and universities should engage their system administrators in annual training for technologies emerging in the market. This will equip them with the necessary skills and be ready to combat cyber space crimes..

4.0 CONCLUSION:

Despite the remedies to alleviate problems of access to Internet and regulation, the problems continue to expand and manifest themselves. As technology grows, different countries need to develop and explore the existing laws to suit new technology. In most instances, Internet being a medium of communication just like other media, the laws that apply to them should also be extended to it. By establishing Internet laws and policies, the qualities of the Internet will greatly determine them. Internet laws and regulations alone are not enough; moral ethics is required for all the users who operate under it in the world. System administrators, IT managers and computer professionals should have a code of ethics as they execute their duties on the Internet. To help in Internet regulation, computer administrators should:

a) Develop ethics and security policies to computers.
b) Develop a computer ethics guide.
c) Find and expand a business policy to include computer and Internet.
d) Make organizations emails privacy policy.
e) Participate in computer ethics campaign.
f) Manage databanks for organizations.
g) Secure all the passwords for the network

REFERENCES:

[1]. Ackerman E. (1995), "Issues ethical legal security and social," Learning to use the Internet, Franklin And Associates Inc. Wilson Ville, Accessed 2nd Jan.2008.

[2]. Bullesbach, A. (2004). "Current Challenges of data protection in the world Economy." http://www.abkonfereneja.giedo.gor.pl/data/resources/BullesbarchA-Pres-en.pdf. Accessed 23rd December 2007.

[3]. Dickin, J. (2002). " The Internet as a site of citizenship". Canadian Journal of Communication (Online), 27(4). Available: http://www.gc-online .ca/view article. Php? d= 747 Accessed on 24th December 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[4]. Frances, S.G (2002). Some ethical reflections on cyber staking.
[5]. COLUMN: Equal opportunities online. PP 22-32.
[6]. Gianluca E. (2002). "Racist and Xenophobic content on internet Problems and solutions". International journal of communication law and policy. Issue 7 PP 1 – 16.
[7]. Holly Y (2002) Web accessibility and the Law: "Recommendations for Implementations". Library Hi Tech journal (20), 4 pp 406-419
[8]. http://www.emeraldmsight.com/10.1108/07378830210452613
[9]. Horner, D.S (2003). The error of futurism. Prediction and computer ethics. PP 1. http://doi.acm.org/10.1145/968358.968359.
[10]. Johnson, D.G (2000) Democratic values and the Internet Australian journal of information systems PP 1-5.
[11]. Lucas, D.I (2004). "Privacy and the computer: Why we need privacy in the information society" ETHICOMP Journal 96 PP1-13.
[12]. Martin, J.B (2003) Audit and control of the use of the Internet for learning and teaching. Issues for Stakeholders in higher education. Managerial auditing Journal. (18), 3 PPs 244-253. http://www.emeraldinsight.com/10.1108/02686900031046907.
[13]. Pallab, P (1999). "Marketing on the Internet". Journal of consumer Marketing (13), 4 PPs 27-39. http://www.emeraldinsight.com/10.1108/07363769610124528.
[14]. Peter, T. (2002). "The new usability; the challenge of designing for Pervasing computing". Proceedings of the 15th conference on computer communications. PP 382-388.
[15]. Richard, G.P (2005). "Ethical and Social Implications of the internet." http://www.emeraldinsight.com..
[16]. Stephen, D. (2002). "Use of the worldwide Web, hyperlinks and managing news by criminal justice Agencies. Policing. An international journal of police strategies and management (23) 3 PP 318-338. http://www.emerald.library.com.
[17]. Wonnacott, L. (1999) policing the Internet. If your users can't surf responsibly, May have to monitor them. InfoWorld (21), 13 PPs 13-14.