Nigeria cybercrime and ICT development
And Internet Service Provider

Dr. Yakubu Ajiji Makeri
School of Computing and Information Technology
Kampala International University, Uganda
(Yakubuajiji1@gmail.com)

Abstract

The identification of Information and Communication Technology (ICT) as an essential tool for sustainable development has proved to be worth every investment in Nigeria. Unfortunately, 'the country's image' has 'also suffered as a result of the nefarious activities of some Nigerians, who turn the Internet into a cheap channel for the perpetration of criminal activities, ranging from phishing, online trickery and the "Advanced Fee Fraud (AFF)" popularly known as '419 spam'. At the forefront these developments 'Internet Service Providers (ISPs). Despite their many laudable contributions as facilitators of 'Internet usage, ISPs serving Nigeria seem to 'stand aloof or seemingly remain oblivious of the 'damaging implications resultant from the 'use' of their infrastructure for online criminal activities. Using questionnaires, 'we conducted a research to determine the level of awareness of ISPs in Nigeria about intermediary liabilities. The Analysis 'of our findings 'using descriptive statistics 'and 'chi-square 'at p<0.05 'level of significance 'revealed 'that the level of security provided against crime by ISPs are relatively low resulting in a positive relationships between the level of internet crime and the attitudes of ISPs to protecting their networks.

Keywords

Intermediary, ICT, Internet Cybercrime, Nigeria

INTRODUCTION

Within the last decade, the use of the Internet in Nigeria has grown so rapidly with the explosion of Internet Service Providers (ISPs), Internet cyber cafés and access points. This has had several positive impacts on the social, economic and educational sectors in the country [11][17][18]. Unfortunately, the country’s image has 'also suffered as a result of the nefarious activities of some Nigerians, who instead of utilizing the 'Internet 'for productive purposes, turn it into a cheap channel for the perpetration of criminal activities,
especially the 'Advanced Fee Fraud (AFF)' popularly known as '419' [2]. Nigeria has therefore emerged as a source of fraudulent Spam mails characterized by bogus 'business proposals' and 'fraudulent joint ventures. To date, spamming, phishing and other forms of cyber crimes remains one of the most prevalent activities on the Nigerian Internet landscape accounting for the 18% of all online activities amongst others [19][21][12][23][24][26][27]Information released by the United States Internet Fraud Complaint Centre in 2006 brings the Nigerian Spam situation to the fore as the number three among the first ten nations that serve as the source of Spam all over the world [20][22]. The Economic and Financial Crimes Commission (EFCC) is the body empowered by government to fight all forms of financial crimes including cyber crimes in Nigeria. They are working in tandem with the Cyber crime Prevention Working Group.

1.1 Internet Service Provision

Internet Service providers (ISPs) are necessary at every stage of an internet transaction. Even the simplest internet transaction usually involves a 'user's computer, an 'internet service provider's 'access' computer, a 'regional router,' a 'governmental 'backbone' computer, another regional router, another internet service provider's 'computer,' and a 'content provider's computer. So, even in the simplest transactions, there are many more intermediaries than users or content providers [6][7]. To end-users, the ISP is the entity responsible for making access to the content on the internet possible. An end-user is not concerned with which company actually provides the physical network that transmits data across the country or the protocols that ensure that the data gets routed to the right place. But recognizing the importance to appropriate regulatory design of sensitivity to context, it is important to distinguish different roles that ISPs play in common internet activities.

There are three main types of ISPs that are always involved in an internet transaction: Backbone Providers (National ISP), Source ISPs (Regional ISP), and Destination ISPs (Local ISP). The first group includes those that operate solely at the level of transmission (Backbone Providers), with no direct relationship to any of the actors at the 'endpoints' of the 'transmission. Generally when discussing 'cybercrimes' and 'misconducts, the 'Backbone' providers are of relatively 'little interest, because their 'networks' are in 'practice unable to distinguish between different types of data they are carrying. Destination ISPs (Local ISP) serve the end-user who requests content over the 'internet. 'The 'Destination ISP can be subcategorized as Retail ISPs and Link ISPs.

The Retail ISP is the ISP that bills the end-user. The Link ISP provides applications of the internet such as the 'ability to connect to the World Wide Web, who thus serve as gateways for end-users to everything on the internet. As the 'owners' of 'equipment' that 'operates' to 'link networks to the internet backbone, and translate application 'data' into a 'format' that can be transmitted along the 'backbone, these ISPs are well-placed to prevent some 'types of 'harm' by blocking access to certain data available on the internet, or to prevent the transfer of certain other kinds of data such as malicious worms (Jonathan Z., 2003).

Since 'Link ISPs' and 'Retail ISPs always work in together to provide the 'end-user with internet 'access, it is analytically 'necessary to think of their 'functions as either 'integrated or disintegrated depending on 'the 'situation. 'For instance, if a regulation is
directed at preventing certain individuals from gaining internet access, then a focus on Retail ISPs, who deal 'directly with the individuals, is appropriate. By contrast, a 'focus 'on 'Link ISPs 'would 'be 'inappropriate because those actors would find it more costly to identify 'individuals. ' 'If, 'on 'the 'other 'hand, 'a regulation required IP filtering, it would have to be directed to Link ISPs, who handle the internet traffic, rather 'than 'Retail ISPs, 'who 'have 'no technological capability to filter internet traffic. But in other contexts, it is more helpful to view a co-operating Retail ISP and Link ISP as a single entity, the Destination ISP.

The Source ISP, in contrast, may be involved in 'a 'range 'of 'ways 'that 'are 'relevant 'both 'in assessing how “fair” it is to “blame” the Source ISP for the misconduct (the predominant question in existing judicial doctrine) and also in assessing how effectively the Source ISP could serve as a gatekeeper to stop the misconduct (the predominant ‘question ’for ‘us). ' 'For 'example, 'a Source ISP that is providing not only access, but also 'a 'server 'on 'which 'the 'unlawful 'material resides, may be much better placed to monitor and control the 'activity 'than 'one 'that 'provides only access.

Second, 'more 'importantly, 'the 'Destination ISP 'that 'wishes 'to 'serve 'ordinary 'end-users cannot readily remove itself from the jurisdiction of the government in whose territory the users are located. ' 'By 'contrast, 'the 'Source ISP 'that 'is willing 'to 'facilitate 'unlawful 'behavior 'can remove 'itself 'to 'a 'jurisdiction 'that 'does 'not prohibit 'the 'behavior 'in 'question. ' 'Thus, 'for example, 'the 'Source ISP 'that 'is 'willing 'to facilitate internet casinos can make its services available 'anywhere 'that 'local 'laws 'allow 'such activities, putting these entities outside the reach of most 'law 'enforcement 'agencies. ' 'But 'the Destination ISP that provides the connection for customers 'in 'Ohio 'for 'example, 'to 'visit 'the internet 'casino 'in 'Antigua 'must 'be 'present 'in Ohio, if not only in the form of a local server, cable, or router [23].

1.2 Existing Liability Schemes

As a general matter, it is likely that the person who 'can 'efficiently 'prevent 'most 'forms 'of internet-related misconduct is the primary perpetrator. When an internet worm is released onto the internet, for example, the person who can most easily prevent the harm is the person that wrote the worm (the content) and released it onto the internet. For internet 'gambling to be successful, there must be both a gambler and a gambling website. If either of these individuals is lacking, the gambling will not take place. Thus, if either of these actors can be controlled directly, then the social harm caused by internet gambling can be 'prevented. ' 'This 'direct approach is 'the path that the law traditionally has pursued.

But regulation that seeks to prevent misconduct through controlling primary perpetrators is not always effective. These laws are 'ineffective 'when 'individuals 'are 'judgment proof or when prosecution is not efficient either because 'of 'the 'high 'volume 'of 'transactions 'or because 'of 'the 'low 'value 'of 'each 'transaction. Thus, 'to 'use 'the 'obvious 'and 'well-known example, 'direct 'regulation 'of 'individuals 'that share 'copyrighted 'material 'on 'the 'internet 'has not, 'to 'date, 'been 'effective 'to 'significantly decrease that type of conduct.

When targeting primary perpetrators is ineffective, policy makers must choose between allowing 'proscribed-conduct 'harms 'to 'continue unchecked and identifying alternative regulatory strategies. Generalizing broadly, existing policy responses have proceeded along two paths, both of 'which 'have 'resulted 'for 'the 'most 'part 'in 'a relatively 'broad 'freedom 'from 'liability 'for intermediaries. ' 'First, 'in 'a 'variety 'of 'contexts, courts 'have
applied traditional fault-based tort principles to evaluate the conduct of intermediaries. Although there are instances in which relatively egregious conduct has resulted in liability, many if not most of the cases have absolved intermediaries from responsibility. Second, in contexts in which courts have held open the prospect that intermediaries might have substantial responsibility for the conduct of primary perpetrators, Congress has stepped in to overrule the cases by granting intermediaries broad exemptions from liability. The paths share not only the reflexive and unreflective fear that recognition of liability for intermediaries might be catastrophic to internet commerce; they also share a myopic focus on the idea that the inherent passivity of internet intermediaries makes it normatively inappropriate to impose responsibility on them for conduct of primary perpetrators. That idea is flawed both in its generalization about the passivity of intermediaries and in its failure to consider the possibility that the intermediaries might be the most effective sources of regulatory enforcement, without regard to their blameworthiness.

2.0 Internet Crimes

Internet misconducts or crimes refer to the wrongful use of the internet. It involves using contents or services which are prohibited or generally taken as crime. Cyber crime is defined as crimes committed on the internet. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cyber crimes involve two parties; there is the sender and also there is the receiver. Many have blamed the receiver of criminal contents simply because they made reply and give adequate attention to the contents without considering the risks involved in the contents. Internet misconduct may take different shape depending on the level of understanding of the perpetrator and the nature of the business to be transacted in the process.

In every crime committed on the internet, the computer is either a target or used as a tool. For example, cyber stalking and hacking both involve attacking the computer, but the main target of a cyber stalker is the victim, not the computer. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system. When the individual is the main target of the crime, the computer can be considered the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world. Human rather than mechanical weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the perpetrators all the more difficult. The essential concepts and motives have remained largely unchanged. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend [3][4][5]. Summarily, the following forms of internet crimes can be identified among others — software piracy, pornography, spamming (including cyber stalking, phishing, network intrusion, malware, viruses etc)

2.1 Cyber Crime & Criminality in Nigeria

Crime tries to remains elusive and ever strives to hide itself in the face of development. Different nations have adopted different strategies to contend with crimes depending on their nature and extent. Certainly, a nation with high incidence of crime cannot grow or develop. That is so because crime is the direct opposite of development. It leaves a negative social and economic consequence [25]. For Nigeria, in the battle
against cyber crimes, efforts are 'now 'being 'directed 'at 'the 'sources 'and 'channels 'through 'which 'Cyber-crimes 'are 'being 'perpetuated '– 'the 'most 'popular 'one 'being 'Internet 'access 'points 'aided 'by 'insensitive 'ISPs. 'Majority 'of 'the 'Cyber-crimes 'perpetrated 'in 'Nigeria 'generally 'are 'targeted 'at 'individuals 'and 'not 'necessarily 'computer 'systems, 'hence 'they 'require 'less 'technical 'expertise 'on 'the 'part 'of 'these 'criminals. 'The 'damage 'done 'manifests 'itself 'in 'the 'real 'world 'as 'human 'weaknesses 'such 'as 'greed 'and 'gullibility 'are 'generally 'exploited. 'The 'damage 'dealt 'is 'largely 'psychological 'and 'financial. 'These 'crimes 'are 'similar 'to 'theft, 'and 'the 'likes 'that 'have 'existed 'for 'centuries 'offline 'even 'before 'the 'development 'of 'high-tech 'equipment. 'Through 'the 'Internet, 'the 'same 'criminals 'or 'persons 'with 'criminal 'intent 'have 'simply 'been 'given 'a 'tool 'which 'increases 'their 'potential 'pool 'of 'victims 'and 'makes 'them 'all 'the 'harder 'to 'trace 'and 'apprehend [1][20].

The 'Cyber 'criminals 'apart 'from 'his 'own 'mentality 'and 'the 'strength 'of 'his 'motivations, 'needs 'to 'see 'the 'path 'of 'crime 'ahead 'of 'him 'clear 'of 'obstacles. 'If 'every 'single 'individual 'were 'to 'put 'up 'obstacles 'of 'their 'own, 'no 'matter 'how 'small, 'the 'crime 'path 'will 'seem 'to 'be 'far 'less 'lucrative 'in 'the 'eyes 'of 'even 'the 'most 'desperate 'criminal [2]. 'Progress 'in 'the 'fight 'against 'Internet 'pornography 'is 'not 'really 'meaningful 'in 'Nigeria 'except 'in 'few 'cybercafés 'where 'content 'filters 'are 'downloaded 'and 'installed 'to 'filter 'unwanted 'Internet 'content [4][5][12]

On 'the 'other 'hand, 'even 'in 'Cybercafés 'with 'notices 'warning 'against 'pornographic 'and 'spamming 'activities, 'bulk 'tickets 'are 'sold, 'obviously 'meant 'for 'the 'purpose 'of 'sending 'Spam 'mails 'and 'browsing 'sex 'sites. 'Apart 'from 'the 'availability 'and 'usage 'of 'Internet 'facilities 'in 'cybercafés 'for 'pornography 'and 'other 'cybercrimes, 'the 'evolution 'of 'fixed 'wireless 'facilities 'in 'the 'Nigerian 'network 'landscape 'has 'added 'another 'dimension 'to 'the 'cybercrimes 'problem. 'ISPs 'are 'benefitting 'seriously 'from 'this 'in 'formation-seeking 'explosion. 'Interested 'customers 'who 'can 'afford 'to 'pay 'for 'Internet 'connection 'via 'fixed 'wireless 'lines 'can 'now 'perpetrate 'their 'evil 'acts 'within 'the 'comfort 'of 'their 'homes.

The 'challenge 'in 'fighting 'Cyber-crimes 'today 'relates 'to 'the 'fact 'not 'only 'the 'criminals 'are 'benefitting 'from 'cyber-crime, 'service 'providers 'are 'equally 'benefitting. 'This 'is 'simply 'analogous 'to 'the 'issue 'of 'health 'risks 'associated 'with 'information 'technology 'tools. 'Since 'manufacturers 'are 'benefitting 'from 'massive 'purchases 'of 'GSM 'handsets 'and 'iPods, 'they 'stifle 'research 'that 'unveils 'the 'possible 'health 'implications 'of 'unguided 'usage 'of 'these 'equipments. 'Also 'Cyber-crimes 'have 'been 'in 'existence 'for 'only 'as 'long 'as 'the 'cyber 'space 'exists. 'This 'explains 'the 'unpreparedness 'of 'society 'and 'the 'world 'in 'general 'towards 'combating 'them. 'Numerous 'crimes 'of 'this 'nature 'are 'committed 'daily 'on 'the 'Internet 'with 'Nigerians 'at 'the 'forefront 'of 'sending 'fraudulent 'and 'bogus 'financial 'proposals 'all 'over 'the 'world. 'Nigeria 'has 'therefore 'carved 'a 'niche 'for 'herself 'as 'the 'source 'of 'what 'is 'now 'generally 'referred 'to 'as '419 'mails 'named 'after 'Section '419 'of 'the 'Nigerian 'Criminal 'Code (Capp 777 of 1990) 'that 'prohibits 'advance 'fee 'fraud.

2.2 The Nature of Cyber-crimes in Nigeria

The 'following 'categories 'of 'crime 'are 'the 'most 'common 'ones 'in 'the 'Nigerian 'cyber 'space.

(a) Hucksters: 'The 'hucksters 'are 'characterized 'by 'a 'slow 'turnaround 'from 'harvest 'to 'first 'message '(typically 'at 'least '1 month), 'a 'large 'number 'of 'messages 'being
sent to each harvested spam trapped addresses, and typical product based Spam (i.e. Spam selling an 'actual 'product 'to 'be 'shipped 'or downloaded even if the product itself is fraudulent).

(b) Fraudsters: The 'fraudsters 'are characterized 'by 'an 'almost 'immediate turnaround from harvest to first message (typically 'less 'than '12 'hours), 'only 'a small 'number 'of 'messages 'are 'sent 'to each harvested addresses (e.g. phishing, ‘advanced 'fee 'fraud’–419 'from 'the Nigerian 'perspective). 'Fraudsters 'often harvest 'addresses 'and 'send 'only 'a message to them all at a particular time. The major tool for getting addresses is the mailing address extractor [13][14]

(c) Piracy : Piracy involves the illegal reproduction and distribution of software applications, 'games, 'movies 'and 'audio CDs. [9][10][18][16]. This can be done in a number of ways. Usually pirates buy or 'copy 'from 'the 'Internet 'an 'original version 'of 'a 'software, 'movie 'or 'game and illegally make copies of the software available online for others to download and use without the notification of the original owner of the software. This is known 'as 'Internet 'piracy 'or 'Warez. Modern day piracy may be less dramatic or exciting but is far subtler and more extensive 'in 'terms 'of 'the 'monetary losses the victim faces. This particular form of Cyber crime may be the hardest of all to curb as the common man also seems to be benefiting from it[6][7].

(d) Hacking: Young Nigerians can be observed 'on 'daily 'basis 'engaging 'in brainstorming 'sessions 'at 'Cyber 'Cafés trying 'to 'crack 'security 'codes 'for 'e-commerce, ATM cards and e-marketing product sites. The surprising thing is that even with their low level of education or understanding 'of 'the 'intricacies 'of computing techniques, they get results! Phishing 'is 'also 'becoming 'popular 'as criminals 'simulate 'product 'websites 'to deceive 'innocent 'Internet 'users 'into ordering products that are actually non-existent.

2.3 Mediums For Perpetrating Cyber- crimes In Nigeria

The 'Cyber 'criminals 'apart 'from 'his 'own mentality 'and 'the 'strength 'of 'his' motivations, needs to see the path of crime ahead of him clear of obstacles. If every single individual were to put 'up 'obstacles 'of 'their 'own, 'no 'matter 'how small, the 'crime 'path 'will seem 'to 'be far 'less lucrative even in the eyes of the most desperate criminal [1]. Progress is observable in the fight against Internet pornography (except in few cyber Cafés). This is achievable by downloading and installing content 'filters 'to 'filter 'unwanted Internet content [8][9][12]. On the other hand, in 5 Cyber Cafés 'with 'notices 'warning 'against spamming 'activities, 'bulk 'tickets 'are 'sold, obviously meant for the purpose of sending Spam mails. Apart 'from 'the 'availability 'and 'usage 'of Internet facilities in cyber cafes for scam mails and 'other 'cyber 'crimes, 'the 'evolution 'of 'fixed wireless facilities in Nigeria has added another dimension to the Cyber crime problem. Fraudsters 'who 'can 'afford 'to 'pay 'for 'Internet connection 'via 'fixed 'wireless 'lines 'can 'now perpetrate their evil acts within the comfort 'of 'their homes. In some Cyber Cafés, a number of systems 'are 'dedicated 'to 'fraudsters ' (popularly referred to as “yahoo boys”) for the sole purpose of hacking and
sending fraudulent mails. Other Cyber 'Cafes 'share 'their 'bandwidth '(popularly referred to as home use) to some categories of customers who acquire systems for home use in order 'to 'perpetuate 'Cyber-crimes 'from 'their homes.

Efforts at preventing financial Cyber crime in Nigeria are both at entrepreneurial, private and public 'pedestal. 'For 'café 'owners, 'notices 'are pasted 'on 'walls 'warning 'of 'possible 'arrests 'of scammers who send fraudulent mails. Individuals can only take precautions within the limit of the knowledge of the dynamics of the Internet and the e-mail system. Generally, users are learning not to respond to scam mails or mails presenting financial 'bogus 'proposals. 'For the 'government, the Economic and Financial Crimes Commission (EFCC) 'has 'been 'given 'powers 'to 'arrest 'and prosecute individuals and organizations suspected to be involved in the facilitation of Cyber crimes. The bill on Cyber crime has been passed by the National Assembly, it is therefore not unusual to see 'billboards 'donning 'Nigerian 'roads 'warning Cyber criminals that the “hands of the law will soon get to them”. An angle yet to be explored is the ISPs end.

2.4 Primary Perpetrators

Primary 'perpetrator 'offer 'or 'receive content or products over the internet that violates laws related to subjects such as copyright, child pornography, 'gambling, 'and 'trademarks. 'The 'proprietor of a gambling website, for example, offers 'content 'over 'the 'internet 'that 'allows visitors to violate gambling laws. On the other side 'of 'the 'transaction, 'visitors 'to 'a 'gambling website 'receive 'content 'and 'interact 'with 'the content 'in 'ways 'that 'violate 'gambling 'laws. Likewise, a person who introduces a malicious internet 'worm 'onto 'a 'network 'operates 'at 'the 'content layer by putting content onto the web that threatens all computers with internet access. General misconceptions about Nigerian cybercriminals.

Over 'the 'years, 'the 'movie 'industry 'has 'often over-simplified and romanticized the portrayal of the 'cybercriminal. 'Movies 'undoubtedly 'reveal hackers to be misunderstood geniuses attempting to save the very society which ostracized them, only 'to 'be 'impeded 'by 'the 'unforgiving 'harsh government. 'Conversely, 'the 'media 'depicts 'the 'cyber-criminal 'to 'be an 'individual who do 'not believe in the term “free society” hence they are out 'to 'put 'tears 'in 'the 'society 'generally. Logically, the truth lies somewhere in between both images. Most misconceptions people have are unjustifiable. Only an iota of truth exists in them. Cybercriminals do indeed need to be very tech-smart and intelligent to commit crimes and escape scot-free. As with crimes in general, males do form the greater proportion of criminals than women. 'The 'difficulty 'actually 'lies 'in 'dealing with criminals who do not exactly fit the typical profile, easily escaping legal action.

**Misconception 1:** All cybercriminals are smart but social misfits This might have been the case during the time of the standalone computer 'when 'the programmer was usually an a graduate in computing glued in front 'of 'his 'monitor 'and 'punching 'on 'his keyboard. He needed to be very tech-wise and possessed 'little 'time 'to 'socialize 'with 'others. Today, 'however, 'both 'the 'net 'and 'the 'user-friendliness 'of 'personal 'computers 'have 'made committing cybercrimes easy for anyone willing to learn to do so. An effective cybercriminal in the modern-day era needs to have excellent social skills and charisma in order to undertake social engineering 'and 'exploit 'the 'human 'aspect 'of encryption systems.
Misconception 2: Teenagers with computers are all cybercriminals. The media ought to shoulder most of the blame for this stereotype. Countless movies have portrayed individual teenage boys hacking into government databases and doing what trained terrorists failed to do. The image of a boy staying up in the night down at his basement working on his computer and wreaking havoc many miles away is prevalent. Just because hacking has become much easier than before does not translate to teenage boys selling military secrets to rival states. Certainly, there may be a one in a million case of such an incident. However, this is an exception which proves the rule. The furthest a typical teenager will go to is illegally downloading warez software and music from the Internet and copying these onto a CD (piracy).

Misconception 3: Cybercriminals Care Cnot “real” criminals. Strangely, many cybercriminals believe these themselves. This actually gives them the justification to continue committing cybercrimes because these are not “real” crimes. The popularity of online chatting under pretence has reinforced the belief that the cyber world is separate from the “real” one. This encourages criminals to dismiss ethics and morals. Cyber stalking, child pornography, online threats and blackmail are now pressing issues. The crimes themselves are not manifested in the real world, but the damage done is. Many also use the Net to find victims in the “real” world to rape, assault or even murder. An even more terrible counter example for this issue is the rapid spread of cyber terrorism in which computers are being used to disrupt all telecommunication and security systems in a country.

Misconception 4: All Cybercriminals have the same characteristics. Although, some cybercriminals have similar characteristics, it is impossible to treat all cybercriminals as if they were alike because they are not. Each criminal subculture has its very own type of personality and areas of specialty. For instance, a scam artist cannot be put in the same category as a serial killer in a getaway truck even if the damage done appears to be the same. Only when people realize that there is no “typical” cybercriminal will they start taking appropriate action against each specific type, in the process closing all loopholes for cyber criminals to operate or escape through.

2.5. The Victims

Ravi K. in 2004, defined victimology as a very important branch of criminal psychology. It is as important, if not more, to know whom the criminal is likely to target. Preemptive action can only be taken by the law if they know who is likely to commit crime as well as who is likely to be targeted. All criminals at least the intelligent ones will only attack those who exhibit certain vulnerabilities. Cybercriminals are careful about the personalities of those they choose to prey on. We identified four levels of cybercrime victims. These are:

1. The Naïve/gullible
2. The Desperados
3. The Inexperienced and
4. Unlucky people

1. The Gullible

There is no doubt that cybercriminals are most fond of people who are easy to deceive. On a more obvious level, phishers are able to fool such people into buying their scams
or being drawn into legal traps. Usually older people are prone to being scammed as they are more trusting and helpful towards others. On a more dangerous level, however, especially children, believe that the people they meet on the net are as friendly and worthy of trust as real people are. Almost all victims of cyber stalkers or online pedophiles are prone to trusting people and making friends easily. An even more dangerous aspect of this is the dissemination of information regarding propaganda or weapon construction. Gullible teenagers or young adults in countries with unstable political climates can be swayed by such information, leading to heightening of national tension.

2. Desperados (For money or “items”)

Many internet users are desperate for easy ways to make cash. Hence, they easily fall for emails that say things like “Get rich fast!” and follow the instructions in the emails which most others are likely to treat as junk. They are almost definitely led to legal and financial entanglements out of which only the perpetrator will make profits. There are others who are attracted to advertisements related to improving one’s physical image. Ridiculous products such as “cheap, effective breast enlargements” etc. claim to boost their self-esteem at minimum cost. This explains why there are so many of such emails in circulation these days. These adverts are almost certainly nothing more than means to extract credit card numbers and render the reader bankrupt. Cyber stalker victims are almost always children and especially teenagers who are desperate for friendship. They try very hard, often too hard, to make online friends with whom to boost their ego. The result is that they are much more likely to become prey to those who wish to satisfy their sexual appetites and manipulate their victims to this end.

3. Inexperienced

There are a lot of people in the world today whose knowledge of the Net is just enough to chat with their friends and maybe get information from here and there. They are totally incapable of protecting their computers from malicious programmes, hackers and maybe even spam. Worse, they may not even be aware of the existence of such crimes, hence become victims in the hands of the professional criminal. They are usually satisfied with their knowledge and see no need to upgrade.

4. Unlucky people

There are also people who fulfill none of these categories but are just unlucky enough to be at the wrong place at the wrong time, in cyberspace that is. A full-scale of attack or a self-replicating and highly advanced virus can cause great damage to networks or PCs and the individual may not in anyway be blamed. An element of surprise does exist in cyberspace. But it certainly does help to be prepared [24][27]

3.0 Research Design

This study seeks to investigate the level of awareness of liabilities accruable to internet service providers (ISPs) in Nigeria when their facilities are used for internet misconduct. The study was conducted ex post facto using the descriptive survey research design. A descriptive survey seeks to find out certain facts concerning an existing phenomenon. The survey method of investigation focuses on people and their beliefs, opinions, perceptions and motivation and makes it easier for the situation to be described
exactly as they exist.

3.1 Research Questions
From the foregoing, the following research questions emerge:
1) What are the level of awareness of internet intermediary liabilities in Nigeria?
2) What are the effects of government policies and regulations on intermediary activities?
3) What strategies if any are employed by ISPs for controlling misconduct on their network in Nigeria?

3.2 Research Hypotheses
The following null hypotheses were formulated based on the research questions:
H0: There is no significant relationship between the awareness of internet intermediary liabilities and level of misconducts over the internet in Nigeria.

3.3 Study Population
A total of sixty (60) questionnaires were distributed both by e-mail and personal administration to intermediaries in Nigeria. This intermediaries consisted of identified ISPs, offering backbones connections for internet usage only, Network companies offering broadband access for voice, video and data communication and Wireless telephone access companies offering phone communication services only. Out of the distributed questionnaires, 45 were successfully completed and returned.

3.4 Instruments Validation/Reliability
A self-constructed questionnaire titled Awareness of Intermediary Liabilities is the main instrument used to collect data for this study. The questionnaire used contain items grouped into 2 sections. Section A request for the background information of the company (Age, Location, Service Type etc) Section B contained items which sought to examine the level of awareness of their liabilities as intermediaries, effect of government regulations on their activities and strategies used by ISPs for controlling the level of misconducts on their network. The face-validity and content-validity of the instrument were verified by experts in the University of Ibadan. The various suggestions made were used to modify the instrument. The reliability coefficient of the instrument used was (a = 0.82) based on the Cronbach alpha method.

3.5 Method of Data Collection/analysis
Undergraduate students under the supervision of the researchers administered the instrument both by hand and through e-mail to the respondents within southwest Nigeria. Descriptive and inferential statistics were used using simple descriptive statistics such as frequency and percentages and chi-square to test for differences between groups. All the hypotheses were tested at 0.05 level of significance.

4.0 Data Presentation and Analysis
The level of awareness of internet misconducts among users
Question 1: ‘Do you know all your customers (clients)?

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>Yes</th>
<th>No</th>
<th>Indifferent</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF RESPONSES</td>
<td>21</td>
<td>15</td>
<td>25</td>
</tr>
</tbody>
</table>

Question 2: Have you ever taken time to study some of the activities of your customers while they are using your facilities?

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>Yes</th>
<th>No</th>
<th>Indifferent</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF RESPONSES</td>
<td>12</td>
<td>24</td>
<td>9</td>
</tr>
</tbody>
</table>

Question 3: What is your level of knowledge on internet misconduct?

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>Highly Informed</th>
<th>Informed</th>
<th>Not Interested</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF RESPONSES</td>
<td>24</td>
<td>3</td>
<td>18</td>
</tr>
</tbody>
</table>

Question 4: Can you name some of the internet crimes and misconduct you know about as an expert in the internet business?

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>Yes</th>
<th>No</th>
<th>Indifferent</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF RESPONSES</td>
<td>6</td>
<td>36</td>
<td>3</td>
</tr>
</tbody>
</table>

Question 6: Do you have a list of addicted internet users in your network?

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF RESPONSES</td>
<td>27</td>
<td>6</td>
<td>12</td>
</tr>
</tbody>
</table>

Question 9: Is your services 24 hours services?

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>Yes</th>
<th>No</th>
<th>Indifferent</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF RESPONSES</td>
<td>36</td>
<td>6</td>
<td>0</td>
</tr>
</tbody>
</table>

Question 10: If (9) is ‘Yes’, how many staff do you normally have for the night shift?

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>1-5</th>
<th>6-10</th>
<th>11-15</th>
<th>16-20</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF RESPONSES</td>
<td>38</td>
<td>6</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>

Question 11: There is the believe that ISPs pay huge amount of money for monthly bandwidth, is this true?

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>Yes</th>
<th>No</th>
<th>Indifferent</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF RESPONSES</td>
<td>27</td>
<td>6</td>
<td>12</td>
</tr>
</tbody>
</table>

From the tables above, 46.7% of the respondents know the nature of customers they have on their network. 53.3% of the respondents do not know the kind of activities their customers do on their network, meaning they do not monitor the networks. 53.3% of the respondents are highly informed about internet misconducts. 80% of the respondents were not willing to give details about the misconducts committed on their networks. 60% of the total respondents who answered the questions say they have a list of addicted
internet users on their network but do not 'know 'what 'they 'do 'online 'each 'time 'they visit. '80% 'of 'the 'respondents 'offer '24hours services daily for their clients but over 86% of the respondents under-staff their night shifts. 60% of the respondents agreed to the fact that Internet Service 'Providers 'pay 'very 'high 'bandwidth 'to keep their network running.

Effects of Government Policies and Regulations on Internet Intermediaries’ activities

Question 13: Do you know of any law(s) or acts 'that 'are 'enacted 'by 'the 'government 'to regulate the services of ISPs?

![Options Table]

Question 14: If 'answer 'to '(12) 'is '”Yes', 'do you think the law has been able to meet up with the target of sanitizing the internet?

![Options Table]

Question 15: Do you agree to the statement that 'ISP 'should 'be 'liable 'for 'all 'misconducts perpetrated by internet users?

![Options Table]

Over 66% of the respondents say they do not know of any laws or act in the areas of cyber crimes 'or 'cyber 'misconduct. 'Over '86% 'of 'the total respondents disagree to the fact that existing laws have been able to sanitize the cyberspace. Over 86% of the respondents disagree to the fact that Internet Intermediaries should be held liable for crimes committed on their networks.

Strategies Used By ISPS for Controlling the Level of Misconducts on Their Network

Question 16: Rate 'your protective 'measures against internet misconduct

![Options Table]

Question 17: What is the level of security on your network?

![Options Table]

46% 'of 'the 'respondents 'rated 'their 'protective strategies against internet misconducts as ‘below average. '26% 'of 'the 'respondents 'rated 'their network security as strong.

4.1 Hypothesis Formulation

H0: There is no significant relationship between the 'internet 'service 'providers 'and 'the 'level 'of misconducts over the internet. If there is significant difference between the
observed and the theoretical distributions, the chi square test will have to be applied before we can take a final decision on the issue at stake.

<table>
<thead>
<tr>
<th>Observed</th>
<th>Theoretical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Of Users (Age, Gender)</td>
<td>Total</td>
</tr>
<tr>
<td>12-20</td>
<td>40</td>
</tr>
<tr>
<td>21-25</td>
<td>30</td>
</tr>
<tr>
<td>26-30</td>
<td>35</td>
</tr>
<tr>
<td>31-40</td>
<td>24</td>
</tr>
<tr>
<td>41-50</td>
<td>28</td>
</tr>
<tr>
<td>50- and Above</td>
<td>3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>118</td>
</tr>
</tbody>
</table>

Table 4.1: Internet Misconduct

From the table 4.1, the following holds:
The totals are obtained by adding values across a row and a column respectively i.e 40+8=48. The proportion of totals is obtained by dividing each value by the total in a column i.e 48/118=0.22. To obtain the theoretical values, the total of observed values are multiplied by each of the proportion of totals i.e 0.22*118=25.96 for pornographic site. Since there is difference between the totals of the observed and the computed values, the chi-square test is now to be applied using the formula below.

\[ \chi^2 = \sum \left( \frac{f - \hat{r}}{\hat{r}} \right) \]

Resulting in =3.36+5.41+1.23+6.6+9.8+21.55+1.9+5.6+0.29+0.28+10.25+7.6 = 73.68

From degree of freedom df = (c-1)(r-1) where c = total number of columns and r = total number of rows, C =2, r = 6, therefore df = (2-1)(6-1)= (1)(5) = 5

5.0 Results and Discussion

The data presented in this table were gathered from a internet access points using participant observation method of data collection on two major internet misconducts relative to protective mechanisms installed in the various access points based on the level of awareness of the intermediary liability by the owners. The researchers monitored the activities of users at some public internet access points in south western Nigeria over a period of 6 months. The information presented below was observed as the major activities in the cyber café.

Using chi-square distribution table, the chi-square value for the 0.01 level with 5 degree of freedom is 15.086 and for the .05 level, it is 11.071. The computed chi-square value from the results obtained is greater than any of the two table values. Hence the Null hypothesis is rejected and the alternate hypothesis is accepted. We therefore accept that:

H1: There is significant relationship between the awareness of internet intermediary liabilities and level of misconducts over the internet in Nigeria

6.0 Concluding Remarks

The internet is coming of age. Though at the advent of the internet it may have been necessary to develop laws and policies that protected the fertile ground in which the businesses and technologies of the internet have grown, today the internet has taken hold and permeates our daily lives. Companies that provide access to the internet as well as companies that provide content on the internet are becoming entrenched in their positions
of dominance. Non-internet companies have also incorporated the internet into their business models to increase efficiency and customer service. At the same time, however, harm perpetrated over the internet continues to grow each year. The pirates have arrived on the high seas of the online world and the lack of regulation makes collecting their booty all too easy. For Nigeria to reap the gains of development accruable from ICT and especially the global highway, the time has come for lawmakers to implement sensible policies designed to reign in the pirates while minimizing the impact on law-abiding users of the internet.

Fighting cybercrime must be a collaborative effort, which will benefit from using tools and standards that aid in exchanging information and performing coordination. To this end, standard methods of reporting spamming events, of characterizing particular spam, and of sending spam control data can be helpful. Some work in that direction should be encouraged. Fighting spam also requires global operations collaboration; this will be aided by services to facilitate interactions between network administrators speaking different languages as well as law enforcement agencies across nations. It is also likely that there should be standards for the syntax and semantics of whitelists and blacklists in inbound mail filtering systems.

It is obvious that there are lots to be done in the areas of finding adequate legislation on internet misconducts and liability of intermediaries in Nigeria. The fact that internet service providers are making undue gains from exploiting these dirty tracks remains a battle that will take more than wits to win. Deliberate legislative activities, backed up by aggressive law enforcement will be a potent method to win the battle against misconduct on the internet in Nigeria. Nigerian organizations today must first and foremost defend their own systems and information from attack, be it from outsiders or from within. They may rely only secondarily on the deterrence that effective law enforcement can provide. To provide this self-protection, organizations should focus on implementing cyber security plans addressing people, process, and technology issues. Organizations need to commit the resources to educate employees on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology such as firewalls, anti-virus software, intrusion detection tools, and authentication services throughout the organizations computer systems. The Internet community must engage in a collective effort to curb the Internet of the demeaning crimes it is helping to fuel. Of course, the damaged and dented image of the Nigerian Internet users remains an issue of concern as a result of the fraudulent mails emanating from our nation.

References