October 29, 2010

CYBER CRIMES; OBSELETING THE GUNS, BOMBS AND KNIVES

Chinedu Chibueze Ihenetu-Geoffrey

Available at: https://works.bepress.com/chinedu_ihenetugeoffrey/4/
It is of no doubt that electronic commerce holds the key to present and future
global and local economic and social growth. However, like every other concept
of human invention, e-commerce has some undeniable teething problems that
tend to bedevil its full applicability. This paper hopes to throw light on some of
these challenges. It does not claim to be exhaustive; rather it is only a guiding
light for further research.

**CYBER CRIME**

‘Crime is always a by-product of an innovation or invention’¹

Cyber criminal activities started with the evolution of the internet and other
technological innovations of our day. One undeniable feature of the internet is its
speed, ease and breath. This very advantage is what cyber criminals have
capitalized on to swindle unsuspecting users of huge resources.

Before delving deeply into the core of this subject, it is pertinent to attempt a
definition of what cyber crime is. A simple but compact definition is ‘unlawful

---

¹ A student of the Lagos State University, Ojo, Lagos State and the Editor of De Quintessence, The
Nigerian Law Students’ Journal
² Baron Verulam of Verulam and Viscount of St. Albans 1561-1626 (an English Philosopher)
acts using the computer as either a tool or target or both.\textsuperscript{3} A broader definition was given in the Telecommunications and Postal Offences Decree.\textsuperscript{4}

“any person who \textit{inter alia} engages in computer fraud or does anything relating to fake payments, whether or not the payment is credited to the account of an operator or the account of the subscriber is guilty of an offence”

Furthermore, cyber crime has also been regarded as computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.\textsuperscript{5} Internet crime has been further given a working definition thus; an act committed by use of the internet (one host communicating with another host) which is classified as a criminal offence according to national law\textsuperscript{6}

Criminal activities on the internet range from fraud, theft, pervasive pornography, pedophile rings, drug trafficking to cyber extortion, hacking etc.\textsuperscript{7} The severity and effect of cyber crime on business, society and government is unquantifiable. Annually, over $1.6 trillion is lost to cyber criminals.\textsuperscript{8} Cyber crime is attracting more attention by the authorities for various reasons;

\textsuperscript{4} Section 2A (h), 1995
\textsuperscript{5} Dr. Gupta and Agrawal \textit{CYBERLAWS} pg 54
\textsuperscript{6} Inger Marie Sunde, Research Fellow http://www.uio.no/studier/emner/jus/jus/ICTLECOMM/v08/undervisningsmateriale/Cybercrime
\textsuperscript{7} P. Williams ‘Organized Crime and Cyber- Crime: Implications for Business’
\textsuperscript{8} Per Little (2006)
1. Money can be transferred through the internet. This is achieved through online electronic payments, such as credit or cash cards, electronic money etc.

2. There is no internationally accepted method of verifying the integrity and accuracy of the information that flows through the web.

3. Frauds committed via the internet pose complicated enforcement and jurisdictional problems to investigative agencies and the judiciary.

4. Finally, electronic commerce is here to stay. Despite the myriad of problems yet it is impossible to think of modern commerce without electronic commerce.\(^9\)

**Why break into computers?**

- Hack for pride and fame
- Steal information
- Erase data
- Cause malfunction on the system
- Obtain storage space for pirated goods
- Obtain **anonymity** in order to:
  - Break into another computer (fame & pride / steal info / erase data / cause malfunction etc.)
  - Distribute illegal material
  - Launch a DOS-attack

---

- Send spam
- Phishing attacks

- Create an unauthorized net in order to:
  - Launch a DOS-attack
  - Manipulate lotteries and games by sheer frequency

Just as the elements of traditional crime must be fully present for an accused to be indicted, so also does cyber crime have some specific elements and stages which the prosecutor must establish to convict an accused. These stages include:

(a) **Planning:** at this stage the criminal carefully observes the pattern and trends of the target. This would include his data entry style, programme listing, systems documentation etc.

(b) **Execution:** most computer crimes are executed remotely, thereby eliminating the need for physical presence. Criminals execute their act by modifying application programmes or operating system, accessing controlled programmes etc.

(c) **Concealment:** the criminal having executed his act, deliberately conceals it from being discovered. Cyber crime can be concealed by representing the act as an error or omission, performing the illegal act in conjunction with an authorized activity.

---

10 Inger Marie Sunde, Research Fellow
[http://www.uio.no/studier/emner/jus/jus/ICTLECOMM/v08/undervisningsmateriale/Cybercrime](http://www.uio.no/studier/emner/jus/jus/ICTLECOMM/v08/undervisningsmateriale/Cybercrime)

11 *Mens Rea*—mental element and *Actus Reus*—physical element.
(d) **Conversion**: the criminal has to convert the criminal object into tangible object of use to him. Conversion can take place in different means, sale of data unauthorizely acquired, destruction of data in cases of revenge, or in most cases for the financial gain.\(^{12}\)

The New Jersey Star Ledger reported\(^{13}\) that a 13 years old boy used his parent’s auction account with eBay (an online Auction company) to successfully bid on $1.2 million medical centre in Jacksonville, Florida and another $400,000 bedroom suite that once belonged to Sir John A. Macdonald-Canada’s first prime minister.

**CLASSIFICATION OF ELECTRONIC COMMERCE FRAUDS**

**Consumer-type fraud**: this is perpetuated through internet auction frauds, health care products sales; travel and tourism services.

**Investment-type fraud**: this is perpetuated through pyramid selling schemes, ‘pump and dump scam’, ‘risk free’ marketing, off-shore frauds etc.

**Business-type fraud**: this is actualized through online payment and manipulation of data fraud and the usage of Net fraud. It is achieved through manipulation of internet access services, international modem dialing and web cramming.\(^{14}\)

---

**TOP INTERNET CRIME ACTIVITIES IN 1999 AND 2000**

---

\(^{12}\) Dr. K.P.C Ghandi *An Introduction to Computer Related Crime*

\(^{13}\) Reported on April 28 1999

\(^{14}\) *ibid*
<table>
<thead>
<tr>
<th></th>
<th>1999 Top 10 Frauds</th>
<th>%</th>
<th>2000 Top 10 Frauds</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Online Auctions</td>
<td>87.0</td>
<td></td>
<td>Online Auctions</td>
<td>78.0</td>
</tr>
<tr>
<td>2 General Merchandise Sales</td>
<td>7.0</td>
<td></td>
<td>General Merchandise Sales</td>
<td>10.0</td>
</tr>
<tr>
<td>3 Internet Access Services</td>
<td>2.0</td>
<td></td>
<td>Internet Access Services</td>
<td>3.0</td>
</tr>
<tr>
<td>4 Computer Equipment/ Software</td>
<td>1.0</td>
<td></td>
<td>Computer Equipment/ Software</td>
<td>1.0</td>
</tr>
<tr>
<td>5 Work-at-home</td>
<td>1.0</td>
<td></td>
<td>Work-at-home</td>
<td>3.0</td>
</tr>
<tr>
<td>6 Advance Fee Loans</td>
<td>0.2</td>
<td></td>
<td>Advance Fee Loans</td>
<td>2.0</td>
</tr>
<tr>
<td>7 Magazine Sales</td>
<td>0.2</td>
<td></td>
<td>Nigerian Money Offers</td>
<td>1.0</td>
</tr>
<tr>
<td>8 Information Adult Services</td>
<td>0.2</td>
<td></td>
<td>Information Adult Services</td>
<td>1.0</td>
</tr>
<tr>
<td>9 Travel/ Vacations</td>
<td>0.1</td>
<td></td>
<td>Travel/ Vacations</td>
<td>0.5</td>
</tr>
<tr>
<td>10 Multi-Level marketing/ Pyramids</td>
<td>0.1</td>
<td></td>
<td>Credit Card Offers</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Source: Internet Fraud Watch ([www.fraud.org](http://www.fraud.org))

A list of possible internet crime is inexhaustible; however a few would support this line of thought.

- **Identity theft**- the criminal either steals the victim’s information or card and goes ahead to pose to a seller that he is the owner for payment
purpose. The closest provision of our law relating to this act is in S. 419A of the Criminal Code which provides \textit{inter alia}

\begin{quote}
\textit{any person who by false pretence or by means of any other fraud obtains credit for himself or any other person- in incurring any debt or liability; or by means of an entry in a debtor and creditor account between the person giving and the person receiving credit, is guilty of a felony….} The truth is that even this section cannot successfully nail a cyber criminal in view of the intricacies involved in electronic commerce.
\end{quote}

The Advance Fee Fraud and Other Fraud Related Offences Decree\textsuperscript{15} were enacted to ease the proof of this crime. Furthermore the Economic and Financial Crimes Commission is now charged with the responsibility of enforcing Decree No. 13 1995.

- **Cyber Pornography:** this includes pornographic websites including transmission of images of children; pornographic magazines using computers and the internet, dissemination of pornography etc. The American case of \textit{State of New York v. Buffnet}\textsuperscript{16} an ISP\textsuperscript{17} pleaded guilty to the misdemeanor charge of knowingly providing access to child pornography. Investigation revealed that the ISP hosted a pornography newsgroup called ‘Pedo University’. The police warned the defendant but

\textsuperscript{15} No. 13 of 1995
\textsuperscript{16} \textit{State of New York v. Buffnet}
\textsuperscript{17} Internet Service Provider
it refused to comply, after which its servers were ceased and it was made to remove the pictures and pay fine. The Convention on the Rights of a Child guarantees the right of protection of children against pornography and obscenities.

A learned author puts it in perspective thus;

“…. The latest trend seems to be towards interactive ‘LIVE SEX’ where people perform on and according to requests by subscribers to the services. The end user can view all of these on his computer, save and transmit it or printout hard copies of images and text.”

- **Internet Matrimony:** Marriage and relationships are largely built on communication between two willing adults. The internet offers an unprecedented communication platform for such issues. The story was told of one Anastasia Solovieva of former Soviet Union who was matched with a fat, elderly man (Indle King Jr.) who had been a former tug earlier convicted of violence upon his earlier internet gotten wife.

Two years after the marriage, Anastasia was found dead, strangled and buried in a junkyard by her husband. Internet matrimony is gradually filtering into Nigeria with the recent report of an American lady who met her bricklayer husband in the chat room. Time will tell how well such marriages

---

18 Ratified and domesticated by Nigeria via section 12 of the 1999 Constitution.
19 Shri Dev. Gangjee *Pornography on the Internet and the Indian Penal Code* pg 259
would work. A lot have turned out to be charades in which one of the parties knowingly induces the other for a personal advantage.

- **Sale Of Illegal Or Stolen Goods:** the internet offers a gateway for the sale of goods through auction, mail-order or directly to the buyer. These goods include but not limited to hard drugs eg. Cocaine; body parts eg kidneys; by-product of endangered species, ammunitions, stolen goods etc section 427 of our Criminal Code criminalizes reception of stolen goods. The elements of such successful charge include;

  1. The theft of the goods
  2. The goods were taken into possession by the accused.
  3. At the time of receiving, the accused knew that the goods were stolen\(^\text{21}\)

The Endangered Species (Control of International Trade and Traffic) Act controls the sale of animal species threatened with extinction. The Economic and Financial Crimes Commission (Establishment) Act\(^\text{22}\) also makes it an offence to own or sell or buy narcotic drugs.

- **Piracy, Copyright Infringement, Trademark Violations:** the case of

  *Playboy Enterprises Inc. V. Frena*\(^\text{23}\) operator of a bulletin board allowed its subscribers to upload and download digitized pictures copyrighted by

---

\(^{21}\) See also section 268 Criminal Code  
\(^{22}\) No. 5, 2002  
\(^{23}\) 839 F. Supp. 1552 (M.D. Fla 1993)
‘playboy’ magazine. He was held liable for infringement notwithstanding that he claimed ignorance and promptly removed the pictures on knowing.\textsuperscript{24} So many other intellectual property crimes could still be committed by a person. This includes software piracy, trademarks violations, theft of computer source code etc in Nigeria the only regulation that can be construed to nail infringers is the Copyright Act\textsuperscript{25} or case laws

- **E-Mail Spoofing:** This is when an e-mail appears to originate from a source but which actually did not. A good example was given by a learned writer.\textsuperscript{26} In India, a Pune based businessman received an e-mail from the Vice President of the Asia Development Bank (ADB) offering him a lucrative contract in return for a large sum of money. The victim verified the e-mail from the website of ADB and found it correct so he sent the required amount into the specified bank account. It later turned out that the e-mail was actually sent by a *Nigeria based Indian!*

- **Cyber Defamation:** Defamation was defined by section 142 of Shariah Penal Code of Zamfara state as spoken or reproduced words by mechanical means intending to harm or knowing or having reason to believe that such imputation will harm the reputation of a person.\textsuperscript{27} The

\textsuperscript{24} See also *Frank Music Corp v. Compuserve Inc.* (No. 93 Cir 8153 S.D.N.Y 1993)
\textsuperscript{25} CAP 68 LFN 1990
\textsuperscript{26} Toun Adebiyi (Mrs)
\textsuperscript{27} See also section 77 of the Criminal Code.
usual question here is who is liable for the defamatory material, is it the author, the host or the ISP? In *Anderson V. New York Telephone Co.* where the plaintiff a bishop was defamed by a client of the defendant who leased a recording machine with which he recorded some information about the plaintiff’s infidelity and account of children born outside wedlock. He sued the telephone company for defamation. It was held that the telephone company cannot be held liable for acts done by its client. Another interesting case is *Stratton Oakmont Inc. V. Prodigy Services Co.*

- **Cyber Stalking:** Stalking has been defined as the crime of following someone over a period of time in order to force them to have sex or kill them. Although no universal definition exists yet cyber stalking has been defined as the use of the internet, e-mail or other electronic methods to stalk or harass a person. One Donald Ridley in UK pleaded guilty to internet stalking. He conducted a campaign against a lady he knew 6 years earlier by setting up a website which invited strangers to rape and abuse her. At a point the victim was receiving up to 30 mails per day including unwanted visitors.

---

28 (1974) 35 NY 2d 746
30 Longman Dictionary of Contemporary English (Third Edition)
31 Occurred in March 2001
- **Hacking**: hacking is an act of securing unauthorized access to a computer or computer network. Hackers are divided into two types—white-hat hackers and black-hat hackers. White-hat hackers are legally employed or independent contractors who hack to check the security of a system. Black-hat hacking is illegal, because such hackers do their activities to cause damage or steal information from the computer or network of a victim. Apart from the above classification hackers have also be classified thus:

1. **Code Hackers** - they can succeed in making the computer do nearly anything they want.
2. **Crackers** - they take pleasure in circumventing Operating Systems and its security apparatus.
3. **Cyberpunks** - they have perfected the act of cryptography.
4. **Phreakers** - they use the internet to commit havoc on the telecommunication system eg. Telephone, TV etc.\(^3\)

Hacking, therefore involves penetrating computer systems, which of course requires security procedures to be circumvented. The hackers have found a wide range of ways to achieve this. In most cases these attacks are done for the challenge and challenge alone. The majority of hackers are

---

\(^3\) *Dr. Gupta and Agrawal  Cyber Laws pg 64*
not motivated by any sense of criminal imperative, but only by a deep
curiosity and a fascination with what they see as the ultimate computer
‘game’.33
Packet sniffing, tempest attacks, password cracking, buffer overflow,
Email Interception, Trojans etc are means through which hackers perform
their nefarious activities. Nigeria like most developing countries has no
sophisticated laws on which to successfully prosecute criminal hackers.
An important issue in hacking is *unauthorized modification of computer
programmes or data*. Due to lack of an appropriate legislation in Nigeria
we could take a cue from our fellow Commonwealth sister India. India
has enacted the Criminal Damage Act (1971)34 this act makes damage or
erasure of computer programmes or data an offence. Property here
implies property of a tangible nature whether real or personal.
Information is an intangible property and as such cannot be destroyed in
the traditional sense. The following cases illustrate the point better.

*Cox v. Riley*35 - The accused was found guilty of criminal damage where
he had erased the programme from a plastic circuit card which was used
to operate a computerized saw for cutting card which was used to operate
a computerized saw for cutting programmed designs. Defence counsel

---

33 Neil Barrett Digital Crime pg 43
34 Precursor to the recent Computer Misuse Act (1990)
35 1986 (83) Cr. App. R. 54
argued that the only ‘damage’ done was to the electronic impulses which made up the computer programme and that since the programme was intangible property, such damage did not fall within the act.

The court held that the accused was not charged with damaging the programme but with damaging the plastic card in which it was housed. It was held that the card itself had been damaged by the deletion of the programme because that action had impaired its value or usefulness which required time and effort of a more than minimal nature to replace it. It was temporarily unable to perform the function it was designed to perform.

Re Whiteley36 Mr. Whiteley hacked into an academic computer system in order to delete, amend and add files. He had considerable computing skills, evidenced by the fact that he detected and deleted a programme which had been launched to track and trap him. It was submitted that the computer discs themselves had not been damaged and that the computer discs themselves had not been damaged and that his activities only affected the information stored on them, which was intangible property and, consequently, that his conduct fell beyond the reach of the act.

36 1991(93) Cr. App. R. 25
The court held otherwise that the computer discs had, in fact, been

damaged because their usefulness had been impaired.

The basic purport of the above is summarized in Section 3 of the

Computer Misuse Act- the requisite intent is to cause a modification to the

contents of any computer;

(a) to impair the operation of any computer,

(b) to prevent or hinder access to any programme or data in any

computer, or

(c) to impair the operation of any programme or the reliability of any

data.

It does not matter whether the intent is directed at any particular computer,

programme or data or programmes or data of a particular kind or at any

particular modification or any modification of any particular kind.

A person while trying to cover up his tracks could attempt to erase data. In *R v. Sinha* 37

A doctor was charged for manslaughter and attempting to pervert the course of

justice. A 30-year asthma patient was given a prescription that induced a fatal

asthma attack through which she died. He then went to covertly modify her

\---

medical record by removing the fact that she was asthmatic. The information was however retrieved from the computer disk.

- **Internet Time Theft:** This is the unauthorized use of the internet time paid for by another person. Section 390 of the Criminal Code provides that every inanimate thing whatever which is the property of any person, and which is movable, is capable of being stolen.

  An offence may also be proved under section 484 of the Criminal Code. It states

  "Any person who, with intent to defraud any person,
  Falsely represents himself to be some other person,
  Living or dead, is guilty of a felony"

- **Web Jacking:** This is the electronic version of hijacking. This occurs when someone forcefully takes over the website of the victim (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

  An incident occurred in the USA where the owner of a children website received a mail that her site has been web jacked. She ignored it, but later started receiving calls from different quarters. The webjackers had replaced a section of the site titled “How to have fun with goldfish”. They replaced ‘goldfish’ with ‘piranhas’. Piranhas are a dangerous flesh-eating
fish. Many children visited and followed the instructions and were injured in the process.

- **Cyber Squatting:** this is the act of reserving a domain name on the internet, thereby denying true users of the name from using it. The Cyber Squatter does this in order to sell such names for cut-throat prices.

- **Email Bombing:** The cyber criminal registers the victim’s email with so many mail service organizations thereby making the person receive hundreds of unwanted emails everyday from different quarters. This can make the ISP to delete the victim from its service.

- **Salami Attack:** this is used to perpetrate financial crimes. The key here is to make the alteration so insignificant that it would be mostly unnoticed. A good example is the case of Ziegler. A bank employee had his employment terminated; he therefore decided to get back at his former employers. He wrote a program which was to deduct 10 cents from every account and dump in the account of the last person on the customers list every Saturday. He therefore opened an account in the name of Ziegler. This went on for a long time until another person actually bearing the name Ziegler opened an account and noticed the unusual deposits. He
therefore reported the case to the bank and it was later discovered and prosecuted.\footnote{Toun Adebiyi – \textit{Internet Crime} Capital Market, Law and Economic Development Journal (2004) pg 82}

- **Denial of Service Attack**: this usually involves a malicious flooding of commercial websites, causing them to crash and preventing genuine customers from patronizing the site. There is another variant called Distributed Denial of Service Attack. This is a concerted effort of different people from different parts of the world towards one system or network. It is a little difficult to prosecute this crime. However the European Convention on Cybercrime has provided a leeway in its Art. 5.

  It is criminal ‘\textit{...when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data}’

- **Worm Attack**: a ‘worm’ is a self-replicating programme which eats up space capacity within computers. Worms are found in networks where they infect all the computers connected to the main server.

- **Virus Attack**: a computer virus as the name implies is analogous with medical viruses. A virus in cyber crime parlance is the computer ‘machine code’ that copies its code into a host programme when the programme is
run. Viruses also duplicate themselves depending on the make up.

Viruses are contacted through the use of electronic storage devices, downloaded data from the internet or through file transfer on a select network. Viruses can be classified in two ways;

(i) According to how they attach themselves to the host programme.

(ii) According to their activity

According To How They Attach Themselves To The Host Programme.

The following are types of viruses that have unique manifestation in how they attach themselves.

(a) **Shell**- this forms a shell around the host programme and gain ascendance over the host programme. This makes the original programme sub-program of the virus code.

(b) **Add-on** – these viruses add their own code either to the end or beginning of the host programme.

(c) **Intrusive**- these viruses replace the host programme code with their own code.

According To Their Activity
(a) **Boot** – this affects the booting of the system. This hinders the system from storing vital information necessary to load the operating system which helps the computer to start up.

(b) **Programme**- this virus infects executable programme files. They usually have extensions like .exe, .com, .sys, .drv. When the programme is executed it spreads to the files.

(c) **Macros**- this virus infects the macros of the Microsoft word documents and templates. The virus travels along with the document and infects other computers also.

(d) **Polymorphic**- this virus appears in different forms in different infections as it has the capacity the capacity to change its code. This is very difficult to difficult.

(e) **Zoo**- this is an experimental virus that is confined to a research lab.

- **Trojan Horses**: Trojan horses don’t usually replicate themselves; instead they hide their true intent behind something benign. They can present themselves as games, programs, screensaver etc. Trojan horses are designed primarily to give hackers remote control of the victim’s computer. They also engage in other sinister acts;

  (i) They could send themselves to everyone in the victim’s address book.
(ii) they may erase or alter the victim’s files

(iii) They may steal data including credit card details.

(iv) They may install a virus or download other unwanted programs.

- **Logic bombs**: these are malicious programmes that are primed to start operating at some point in the future; the trigger can be a specific date or event.

A sacked network administrator in the US was charged after he planted a logic bomb in the system of the company. This cost the firm an estimated $10 million in damage.

**AN APPRAISAL OF EUROPEAN CONVENTION ON CYBERCRIME (ETS 185) NOVEMBER 2001**

Although this is an “European convention” (ETS), yet it is open to third parties.

Three specific chapters regulate the following:

- Criminal law

---


40 Art. 37- This usually occurs when European citizens engage in business activities with non-Europeans.
• Procedural rules ("computer investigation")
• Principles of International cooperation
  • Supplementary to other conventions (art. 39) such as the European convention on Extradition, and
  • On Mutual Assistance in Criminal Matters, and
  • The Additional Protocol to the above mentioned convention.

Cybercrime convention: Criminal law:

• Illegal Access (computer intrusion)\textsuperscript{41}
• Illegal interception\textsuperscript{42}
• Data interference\textsuperscript{43}
• System interference\textsuperscript{44}
• Misuse of devices (exploits and passwords)\textsuperscript{45}
• Computer-related forgery\textsuperscript{46}
• Computer-related fraud\textsuperscript{47}
• Offences related to child pornography\textsuperscript{48}
• Offences related to infringements of copyright and related rights\textsuperscript{49}.
• Attempt / aiding / abetting and corporate liability\textsuperscript{50}

What is not covered by the convention?

• Information theft.

• Information fencing (laundrying) and self laundrying.

• Scanning activities.

• Identity theft.
• Spam.

\textsuperscript{41} Art.2
\textsuperscript{42} Art.3
\textsuperscript{43} Art. 4
\textsuperscript{44} Art.5
\textsuperscript{45} Art.6
\textsuperscript{46} Art.7
\textsuperscript{47} Art.8
\textsuperscript{48} Art.9
\textsuperscript{49} Art.10
\textsuperscript{50} Art.11-12
CYBER CRIME CONSIDERED FROM A RELIGIOUS PERSPECTIVE

A lot of issues raised in internet related crimes are of grave concern to a lot of people who hold moral views especially based on religious perspectives. Social norms arise basically from the religious instructions. That is why before stealing was termed criminal, it had been termed a transgression of the Ten Commandments. Issues such as privacy, intellectual property, defamation etc are all issues addressed by major religious groups in the world; these are also major issues in cyber crime.

Some people may argue that our rights of privacy are “socially constructed,” meaning that they change over time under the influence of many human forces and institutions, including technology, culture, and law. Another factor that affects our rights is the strength of the arguments that we use to think about them. Lavine (2001) presents the following ten factors relating to privacy which I feel serves the argument for presenting a discussion about computer crime from a Judeo- Christian and Islamic point of view (Yousif, 2002), these factors are:

1. **Freedom**: Being able to conceal our behavior from others protects us from punishment, discrimination at work, social ostracism, and unpleasant criticism.

2. **Property rights**: Perhaps information about me belongs to me, just as anyone's body is his or her property.

---

51 See Exodus Chapter 20 Verse 15
3. **Informed consent**: As a general matter, we should not do things to others without their permission.

4. **Personality development**: Perhaps we need opportunities for private reflection and experimentation if we are to develop complex personalities.

5. **Avoidance of discrimination**: Powerful people sometimes want to act on the basis of morally irrelevant information.

6. **Avoidance of defamation**: It can be harmful for people to accuse their fellow citizens of misconduct, especially when their accusations are either false or unsubstantiated.

7. **Happiness**: Although there are other moral values besides happiness (consider justice, fairness, compassion, and freedom), we generally think that it is right to make people as happy as possible, at least all else being equal.

8. **Equality of power**: Knowing information about people is a source of power. Protecting the rights of ordinary people to withhold information strengthens them against governments and large firms.

9. **Separation of zones**: Many people believe that it is important to keep society carefully divided into zones such as that of the market, the family, the military, religion, politics, scholarship, and social relationships.

10. **Rights of association**: We have both legal and moral rights to associate in voluntary groups.

    The Bible’s stand on cyber criminal activities is expressed in various parts, however for academic purpose I would consider the widely known Ten Commandments.
Thou shalt not steal\textsuperscript{52} - Information theft; identity theft, salami attack etc are all examples of modernized stealing methods using the computer.

Thou shalt not bear false witness against thy neighbour\textsuperscript{53} - Lord Atkins in the famous \textit{Donoghue v Stevenson Case}\textsuperscript{54} asserted that my neighbour is that person who will be directly or remotely affected by my action or inaction. Therefore the acts of Cyber stalking, cyber defamation etc all run fowl of this biblical injunction. Anyone who is directly or indirectly affected by such act is one’s neighbour.

Thou shalt not covet thy neighbour’s house… nor anything that is thy neighbour’s.

This commandment goes to the root of most cyber criminal motives. Covetousness propels majority of the top internet crime activities stated above. Nigerian money letter\textsuperscript{55} for example is an apt example of covetousness on the part of the target and the perpetuator. In a recent report on the internet, a man who claims to be a pastor (but actually a swindler) was ‘conned’ by an internet group that specializes in bursting ‘419ers’. The man was made to put a big loaf of bread on his head, a wine in his hand and made to sit down in a funny-looking way.

This picture and story was shared with a lot of people via email\textsuperscript{56}

It is trite at this junction to quickly consider some basic concepts especially from the Islamic law perspective.

\textsuperscript{52} Exodus 20v 15
\textsuperscript{53} Exodus 20v16
\textsuperscript{54} (1932)All ER Rep. 1,(1932)AC 562
\textsuperscript{55} Popularly known as ‘419’, after the relevant section in the Nigerian Criminal Code.
\textsuperscript{56} This author received one
Shar’iah\textsuperscript{57} has a very high level of proof for the most serious crimes and punishments. If proof is not as specified then the crime must be considered a lesser crime. The major myth is that judges in Islamic nations have fixed punishments for all crimes. The judge under Shar’iah is not bound by precedents, rules, or prior decisions as in English common law. Hadd crimes, the most serious crimes in Shar’iah law, are murder, apostasy, making war upon Allah and His messengers, theft, adultery, defamation, false accusation of adultery or fornication, robbery and consumption of intoxicants. These are considered crimes against Allah. Tazir crimes are acts which are punished because the offender disobeys Allah’s law and word. Tazir crimes are crimes against society. A Qesas crime is one of retaliation. If you commit a Qesas crime, the victim has a right to seek retribution and retaliation.

**Adellah\textsuperscript{58} for Privacy, Trust, Theft and Promise\textsuperscript{59}**

<table>
<thead>
<tr>
<th>Statement</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALLAH said: &quot;Allah commands you to give back the trusts to their rightful owners&quot;</td>
<td>(An-nessa, 58).</td>
</tr>
<tr>
<td>ALLAH said: &quot;O believers! Do not betray the trust of Allah and His Prophet, nor violate your trusts knowingly&quot;</td>
<td>(Al-Anfal, 27).</td>
</tr>
<tr>
<td>Prophet Mohammad (peace be upon him) said: &quot;The signs of a hypocrite are three: Whenever he speaks, he tells a lie. Whenever he promises, he always breaks his promise. If you trust him, he proves to be dishonest. If you keep something as a trust with him, he will not return it.&quot;</td>
<td>(Al-Bukhari, 1987).</td>
</tr>
<tr>
<td>Prophet Mohammad (peace be upon him) said: &quot;Give back what you have been trusted with and do not betray those who have betrayed you&quot;.</td>
<td>(Al-Hakeem, 1990)</td>
</tr>
<tr>
<td>ALLAH said: “O believers! Do not consume one another’s wealth through unlawful means;</td>
<td></td>
</tr>
</tbody>
</table>

\textsuperscript{57} The civil and criminal code of justice prevalent in Muslim dominated countries and states. Eg Iran, Saudi Arabia, Zamfara state (Nigeria)

\textsuperscript{58} Adellah is an explanation or exposition of a point in Islamic scholarship.

\textsuperscript{59} Copied from *Cybercrime and the Law: An Islamic View* Mansoor Al-A’ali
POSSIBLE METHODS OF CURBING CYBERCRIMES IN NIGERIA

Government’s Role: The government has a major catalytic and administrative role to curb cybercrime. Nigeria currently has no legislation to curb electronic commerce frauds and cybercrimes. The starting point of any formidable fight against cybercrime is proper legislation. Government has to enact laws governing the carrying on of electronic commerce. The laws should outline the specific duties of each party and the liabilities faced by each party in case of negligence and/or breach of trust. For instance, in the US, though the laws governing electronic commerce are still emerging, there are responsibilities and liabilities placed on the credit card companies, the users and the banks respectively.

Regulatory Authorities’ Role: The Central Bank of Nigeria in its regulatory role has issued CBN regulation on electronic banking.\textsuperscript{60} The Economic and Financial Crimes Commission and other anti-graft bodies have issued regulations on

\textsuperscript{60} Issued in 2001
electronic commerce and more particularly on electronic banking. The Nigerian Deposit Insurance Company (NDIC) needs to ensure a form of insurance for services like Valu Card customers separate from the usual deposit insurance of depositors. CBN could also promulgate standards for the practice of electronic banking in Nigeria. There should be a data repository of electronic fraudsters like ordinary fraudsters. This was what helped foil a credit card fraud.

Jason Diekman (20 year old) stole various credit card numbers and tried three times in one year to make wire transfers with the stolen cards, the credit card company was able to deny access the first two attempts but allowed the third. However, Western Union blocked the wire transfer after checking the hot list of fraudsters on the card company’s database and finding Diekman’s name as a security risk.

**Target’s Role:** Banks and other targets of cyber crime can ameliorate the impact by conducting risk assessment, implementation of controls, policy formulation, customer screening, employee screening, due diligence, ethical and professional practice.

In conclusion, cyber crime is a major threat to the growth of internet based commerce and globalization. With over $1.6 billion lost to cyber crime every

---

61 Abstracted from MODUS International Law and Business Quarterly (June 2002), pg 87-91
the least our nation can do is to proactively enact laws on internet transaction regulation, cyber crime etc. fellow African nations have done this and much more. Nigeria as the so-called ‘Giant of Africa’ cannot afford to sleep through the revolution especially in view of the active participation of Nigerians in internet based operations.

---


63 Mauritius: Electronic Transaction Act (2002), closely modeled after the UNCITRAL Model law on E-commerce.

Tunisia: Electronic Exchanges and Electronic Commerce Bill. This covers the use of electronic contracts, signatures and establishing a certification authority and process.

Cape Verde: Passed a law covering use of e-contracts, signatures and the admissibility of electronic evidence in courts in year 2000.

South Africa: Electronic communications and Transactions Act 2002

Egypt: Adopted the UNCITRAL E-signature law in (2004)