INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Addressing Cyber-Harassment as an Electronic Crime against Persons in Nigeria: From Theory to Practice

Dr. Bernard Oluwafemi Jemilohun
Senior Lecturer, Ekiti State University, Ado-Ekiti, Nigeria

Abstract:
Harassment generally is the act of bothering or annoying someone in a constant or repeated way. This unkind and hostile pattern of behaviour has unfortunately found its way into cyberspace. While physical harassment may be easy to cope with by avoiding the cause or agent of the harassment or reporting to physical law enforcement agencies, cyber harassment has not been easy to deal with the same way. The possibility of anonymity in cyberspace and the availability of anonymizers have made the concept of cyber-harassment more difficult to handle. While the advanced nations have made moves to curb this, Nigeria and many African nations have not responded with the same zeal with which the technological advanced nations have confronted the menace even though a pocket of legislations have been enacted to curb the ill. Yet, the impact on the victims in this side of the globe is as damaging as it is in the advanced countries. This paper attempts to appraise the legislative framework addressing cyber-harassment in Nigeria with a view to making suggestions for improvement in the light of the practice in other jurisdictions. The paper concludes that beyond legislation, real practical steps should be taken to ensure that the menace does not take root in Nigeria.

Keywords: *Cyber-harassment, cybercrime, revenge porn, cyber-stalking*

1. Introduction

The concept of cyber harassment has become more prevalent with the increasing use of technology across the globe.[i] (Kamal, 2005) The public accessibility of the internet and other means of electronic communication have made it easier for human beings to interact in more positive and negative ways than before. Much as communication has become easier because of the internet and profitable and meaningful relationships have been forged and strengthened (both in the public and private spheres), negative-minded people have also discovered the other uses the internet may be put to in furtherance of their patterns of committing wrong.

Unlike physical bullying or harassment where the victim can walk away or report the bully directly to physically accessible authorities or law enforcement agents, cyber harassment takes a more technical dimension because more often than not, the offender may not be within immediate reach or may not even be easily identifiable. Though harassment in cyberspace is not much pronounced in Nigeria, recent happenings across the globe and in Nigeria show the need for effective legislation and serious efforts to prevent same. One may tend to think that he or she cannot be harassed in cyberspace, but that may only be if one has absolutely nothing to do with and on the internet. The moment a person begins to live in an environment that is technology conscious and one engages technology in communication, anyone can become a victim of cyber harassment. And there is no limit to the extent that the cyber offender may go in stalking and harassing the victim. A more serious dimension of this offence is revenge porn[ii] which has begun to attract serious attention across the globe.[iii]Revenge porn happens by the posting of real or doctored intimate pictures or video of a person without their consent and in a way to offend, or annoy or intimidate or put the victim in bad light before people.

In the language of the Oxford Cyber Harassment Research Symposium, "Cyber harassment is a relatively new phenomenon resulting from technological advancement and the widespread use and acceptance of technology among people. Cyber harassment is the unsolicited and repeated use of electronic information and communication devices such as email, instant messaging, blogs, chat rooms, cell phones, gaming systems and defamatory websites to bully or otherwise harass an individual or group through threats, intimidation and humiliation. Unlike physical bullying, where the victim can walk away, technology now allows for continuous harassment, from any distance."[iv]

Sadly, more than many people think, the effects of cyber harassment when unchecked may lead the perpetrator to engage in more sinister and malicious acts toward the victim and the effect of this can be deep and far reaching in damaging the emotional well-being of the victims. Sometimes, it can affect a person's performance in his job and even affect their domestic and family life. Some journalists have been forced to backpedal from investigating an otherwise revealing story. And in some more serious cases, it has caused the victims to commit suicide. The developments in the information communication technology sector has enabled both positive and negative dimensions of interaction and conducts. It becomes important that adequate legislations and proper enforcement mechanisms be put in place to curb the menace.

In the light of the evidence from the surrounding nations, no nation should wait until anti-social behaviours made possible by technological advances becomes a source of crime before such matters are addressed. While nations and societies are encouraged to embrace information communications technology, there is the constant need to ensure that laws have the necessary capacity to regulate the interface between humans and technology and the negative possibilities that emerging technologies may be put to.

And as a sequel to the foregoing, law enforcement agencies should keep abreast of the changes in the technological environment and the responses of the law. Where law enforcement is not equipped to acquire capacity to cope with modernisation, there is a high possibility that internet based and internet enabled crimes and offences may not be effectively tackled.

2. The Concept of Harassment

Traditionally, harassment according to Black's Law dictionary refers to words, conduct, or action (usually repeated or persistent) that, being directed at a specific person annoys, alarms or causes substantial emotional distress in that person and serves no legitimate purpose.[v]The Cambridge online dictionary defines it to be illegal behaviour towards a person that causes mental or emotional suffering, which includes repeated unwanted contacts without a reasonable purpose, insults, threats, touching, or offensive language. The Merriam Webster dictionary defines it as bothering and annoying someone in a constant or repeated way, or to make repeated attacks against another. Though it is not specifically defined in Nigeria's statute books, it will include repeated attempts to impose unwanted communications and contacts upon a victim in a manner that could be expected to cause distress or fear in any reasonable person.

In the United Kingdom for example, the harassment of another person or many others can include a range of offences such as those under the Protection from Harassment Act, 1997, the Offences Against the Person Act, 1861, the Sexual Offences Act, 2003 and the Malicious Communication Act, 1988. It is important to note that beyond the harassment of individuals, closely connected groups may also be subjected to collective harassment. Such a group may be members of the same family, residents of the same neighbourhood, members of the same religious organisation, group of a specific ethnic identity, or those engaged in a specific trade or profession.[vi]

The United Kingdom Crown Prosecution Service outlined a number of circumstances in which harassment can occur[vii]:

- In the context of domestic violence
- When the suspect is personally known to the victim
- Where the suspect does not personally know the victim, but their identity is known
- Where the identity of the suspect is not known
- Where the victim is a target of campaign of extremism (labelling someone a terrorist)

It seems that in the majority of cases of harassment, there is usually a connection between the victim and the suspect even where the victim is unaware of whom the suspect may be though sometimes the connection may be brief. In some cases, the suspect and the victim may have had a very brief intimate relationship[viii] (e.g. a one-night stand) and the victim may not even see the incident as capable of being called a relationship.[ix] Behaviours by the suspect could include things like: frequent unwanted contact, visits to the home or office of the victim, telephone calls, text messages, emails or use of social networking sites; following or watching the victim; sending letters or unwanted gift items; damaging the victims property; boasting that they know the address of other family members or children; burglary or robbery of the victim's home or office; becoming embedded with the victim's life by making contact with their friends and family; threats of physical harm to the victim including sexual violence and physical and sexual assault of the victim.

Thus, harassment generally originates from a malicious intention towards another person with the intention that the victim suffers some distress in his person and it need not culminate in physical danger before it is committed. What counts really is that the aggressor/offender has initiated a pattern of communication which may be verbal or non-verbal that sends signals of emotional discomfort, fear, annoyance, intimidation, anxiety, threats of death or injury, demands for ransom, etc. to the victim Harassment generally can and does take many and different forms. A very common type is sexual harassment. Despite national and international efforts[x] to eliminate sexual harassment, there is no single definition of what constitutes prohibited behaviour. Sexual harassment simply is bullying or coercion of a sexual nature, or the unwelcome or inappropriate promise of rewards in exchange for sexual favours.[xi] This happens when somebody either by insinuations or words or other acts makes sexual overtures to another who is not interested. It is common in the workplace and sometimes in educational institutions where superiors attempt to use either their career positions or supervisory authorities to coerce subordinates to succumb to their sexual overtures.

Harassment can happen anywhere whether at work or at home. Though harassment at the work place is largely committed by people known to the victim, it is nevertheless improper. A common example of harassment at work is a boss who always sets impossible targets or abuses their position by undermining the confidence or humiliating another staff before other people. In such cases, it can take the form of verbal or physical harassment, verbal abuse, social exclusion and isolation.[xii]This type of behaviour may be tolerated by staff in corporate organisations where the offender is the owner of the business or a family member of the business owners. It is nonetheless anti-social and should be resisted or at the least discouraged.

3. The Phenomenon of Cyber-Stalking

Cyber-stalking is a form of harassment that takes place on the internet.[xiii]In the words of Reyns et al.,[xiv] (2012) cyber stalking entails the repeated pursuit of an individual using electronic or internet-capable devices. Repeated pursuits in this sense will normally be in the form of unwanted communication through electronic channels which may be threatening coercive or intimidating. (Hazelwood & Koong Magnin, 2013)[xv] The resultant effect is that a sense of fear, stress, anxiety or intimidation is created in the victim. Victims in some cases lose a sense of control over their own lives not knowing the next step the aggressor may take or the next place or time his acts may manifest. Because of the far and constant reach of electronic channels, the fact that the stalker can access the victim at any time and from any distance can override the victim's personal sense of security thus leading to constant experience of fear.

Some of the ways this is done are through email, telephone calls, short message service, and instant message apps etc. It can also include the use of social networking sites, chat rooms, and other forums facilitated by technology. Practical ways by which people do this on the internet include: locating personal information about a victim; communicating with the victim; as a means of surveillance of the victim; identity theft against the victim by subscribing to services, purchasing goods and services in their name; damaging the reputation of the victim; electronic sabotage such as spamming and sending viruses and tricking other internet users into threatening or harassing the victim.

These methods are by no means exhaustive. The dynamic nature of information communication technology makes room for new ideas of doing both the good and the bad.In July of 2013, New York prosecutors secured an arrest warrant against a New Zealand woman named Jessica Parker who had been cyber stalking a writer named Melissa Anellin for approximately 5 years. One email written in 2009 stated, "You will have much to fear from me in the coming months. This is not over until someone is on the floor bleeding their life away," [xvi](Annese, 2013). Despite the distance, the internet allowed Parker to stalk, threaten, and terrify Anellin on a regular basis, promoting a sense of fear and undermining a sense of control in the victim. Cases like that of Anellin demonstrate the serious harm that can be administered through forms of cyber communication.

4. Internet Revenge Porn

The phenomenon of revenge porn is another embarrassing issue that has recently began to stare us in the face in cyberspace. This is not peculiar to any country as the victims are not restricted to any geographical location. But the legal responses to the menace vary from one jurisdiction to another. Revenge porn (also known as non-consensual pornography) is the act of posting intimate or sexually explicit pictures or videos of another on the internet or sharing the same to others through electronic means without the consent of the object of the videos or pictures. It is immaterial whether the victim created the images or the images were created by the offender. It may be subject to debate whether the word revenge should be included in the terminology as an offender may have no score to settle but merely to extort the victim, hence the term 'sextortion' is used by some people.

Recently, the Nigerian court convicted a man of revenge porn. In Attorney General of the Federation v. Olubunmi Ayan[xvii] the accused person posted nude pictures of his former lover on the Social network site Facebook. The accused had earlier threatened to post the nude pictures in 2017 when the victim said she was no longer interested in the relationship and he requested for payment in the sum of two hundred thousand naira, as inducement for him to rescind his decision. Upon the failure of the victim to pay the sum, the accused posted the pictures. The court sentenced the accused to two years imprisonment and payment of fine in the sum of five hundred thousand naira. Taiwo J, observed that the court was lenient in sentencing the accused as the penalty for the crime under the Cybercrime Act was a Seven million naira fine and imprisonment for a term of three years. The judge however lamented that the law made no provisions for the compensation of the victims. He opined that lawmakers should make such provisions when amending the present law.

While the above is the only known case to the knowledge of this writer, it is possible that there are several other victims who have not reported either due to shame or further threats by the offenders. One may say at this point that proactive steps must be taken to curb the rise of this act as the effect in some cases may lead to the victim committing suicide out of shame and fear. Research shows that its psychological effects can be devastating: according Kamal & Newman (2016),[xviii] 80 to 93 percent of revenge porn survivors report struggling with paranoia, anger and shame after their nude photos or videos are posted without their consent, and another survey[xix] indicates that51 percent of revenge porn survivors have had suicidal thoughts.

5. Crimes against Persons: The Nigerian Legal Framework Before 2015

A crime by nature is an act or omission that violates a law and that renders the doer generally punishable under a law. According to Black's Law Dictionary, a crime is "an act that the law makes punishable; a breach of a legal duty treated as the subject matter of a criminal proceeding". The Nigeria Criminal Code Act[xx] states that "an act or omission which renders the person doing the act or making the omission liable to punishment under this code, or under any Act or Law is called an offence"[xxi]. The Act goes ahead, in the next section, to classify offences into three broad categories; namely, felonies, misdemeanours and simple offences.

Crimes against persons are a category of criminal acts which are committed by direct physical harm or force being applied against persons physically.[xxii] These are different from crimes against the state like treason, or crimes against property or against the public generally or criminal offenses in which the perpetrator uses or threatens to use force. Most of the crimes under this category are rooted in the Offences Against the Person Act, 1861. They include murder, manslaughter, threatening to kill, acts tending to cause danger to life or bodily harm, assaults, child-stealing, attempts to procure abortion, etc. The analysis by division is usually into three categories: fatal offences, sexual offences, non-fatal

non-sexual offences[xxiii]. However, the sexual offences under this Act have all been repealed in England and Wales. They are covered under the Sexual Offences Act 2003.

Within the Criminal Code lies the provisions that deal with a special category of offence against the person that may be committed without any physical contact with the person and yet may do serious damage to the person. The offence of defamation[xxiv]is governed by Chapter 33 of the Code and Section 373 states that "Defamatory matter is matter likely to injure the reputation of any person by exposing him to hatred, contempt, or ridicule or likely to damage any person in his profession or trade by an injury to his reputation. Such words may be expressed in spoken words or in any audible sounds, or in words legibly marked on any substance whatever or by any sign or subject signifying such matter otherwise than by words, and may be expressed directly or by insinuation or irony".

Sections 375 makes the offender guilty of a misdemeanour liable to one-year imprisonment but where the publisher of the defamatory statement knows it to be false, and yet publishes it, he shall be liable for imprisonment for two years. Where the offender publishes or threatens to publish, or to prevent the publication of a defamatory matter with the intent to extort money or other property, Section 376 makes the offender liable for a felony and where found guilty is liable to imprisonment to imprisonment for seven years.

The provisions of the Criminal Code Act in Section 233C and 233D prohibit the spread of pornographic materials to the public. On the face of it, this provision prohibits the public dissemination of pornographic materials generally whether it is consensual or not. Thus, in a way, the law prohibits what is known as revenge porn or the sharing of non-consensual pornographic material. The Act states as follows:

233C. "An article shall be deemed to be obscene for the purposes of this Chapter if its effects taken as a whole is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

"The provisions of this section shall extend to any article of two or more distinct items the effect of any one of which is such as to tend to deprave and corrupt; but nothing in this section shall apply to exhibitions in private houses to which the public are not admitted or to anything done in the course of television or sound broadcasting.

233D.(1) Subject to the provisions of this Chapter, any person who, whether for gain or not, distributes or projects any article deemed to be obscene for the purposes of this Chapter, commits an offence punishable on conviction by a fine not exceeding four hundred naira or by imprisonment for a term not exceeding three years or by both."

Nigeria has recently realized that crimes against persons are not limited to old Criminal Code legislative provisions discussed above. Due to the advances in information communication technology and the need for the law to catch up with technology, new laws are necessary. On the other hand, the penalties imposed for these terribly humiliating offences under the Criminal Code are way too insignificant to serve as deterrents to offenders and would be offenders. A fine of four hundred naira (barely above one dollar) is not strong enough to deter a 'jilted lover' from repeating acts of revenge porn regardless of the damage it does to the person of the victim.

This realisation is partly why the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 was enacted with specific provisions governing aspects of harassment in electronic form. The Act makes elaborate provisions for the offence of cyber stalking in Section 24 of the Act. The main differences are that while the Criminal Code provision deals with publishing by the traditional media, the provision of the Cybercrime Act deals with sending a message or other matter by means of computer systems or network and the penalties under the Cybercrime Act are much weightier and serious. This provision will be examined in detail below.

One may wonder why the need for new legislation to curb cyber harassment. There are five important differences identified (which make cyber stalking a unique crime warranting unique laws)[xxv] (Goodno, 2007) between traditional forms of stalking and harassment and the cyber model:

- A message communicated online can be sent to anyone with internet access, is present immediately, and cannot be taken back or deleted;
- The stalker may be anywhere in the world;
- The stalker can stay anonymous with ease because of the lack of physical contact involved in this crime;
- The stalker may easily impersonate another person to communicate with the victim; and
- The stalker may use third party individuals to contact or communicate with the victim.

It appears in the light of the foregoing that it is better for a nation to make new legislation for this class of offences than modifying or adapting previously existing stalking and harassment statutes because of the emphasis on physical presence in the older statutes.

6. Legal Responses to Cyber-Harassment in Other Jurisdictions

It may be proper at this point to discuss the legislative framework for the prohibition of harassment in the United Kingdom and in the United States with a view to learning from them. The two major legislations against harassment in the UK are the Protection from Harassment Act 1997 and the Protection of Freedoms Act 2012. The Protection from Harassment Act was brought into force on 16 June 1997 and was amended by the Protection of Freedoms Act 2012 to include two new specific offences of stalking, through the insertion of sections 2A and 4A.

The Protection from Harassment Act includes the following provisions: harassment; stalking; fear of violence; stalking - involving fear of violence or serious alarm or distress; breach of a civil injunction; breach of a restraining order and a civil tort of harassment. A court dealing with a person convicted of any offence, including those under sections 2, 2A, 4 or 4A of the PHA, may make a restraining order prohibiting the defendant from doing anything described in the order. This order can be made in addition to a custodial sentence or other sentence. The order can be especially useful in preventing continued stalking and harassment by defendants, including those who are given sentences of imprisonment.

The UK passed legislation to deal with revenge porn in 2015. The legislation allows for the prosecution of someone who publishes or distributes revenge porn and intends to cause distress to a party portrayed in the offending material. This does not mean that revenge porn cases were not being prosecuted before last year. Lawyers successfully made use of existing obscenity laws to prosecute such cases and victims also had civil remedies under the right to privacy. But the Criminal Justice and Courts Act 2015 contains specific provisions relating to revenge porn. The Act in Section 33 dealing with disclosing private sexual photographs and films with intent to cause distress provides as follows:

(1) It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made—

- Without the consent of an individual who appears in the photograph or film, and
- With the intention of causing that individual distress.

These novel provisions are the response of a government that takes the wellbeing of the citizens with all seriousness and engage in proactive legislation to ensure that privacy rights and personal interests are protected despite engagements with technology. The challenge however remains with the attitude of law enforcement to this kind of crimes. It is always the case that law enforcement adjust to changes in the law based on technology. The report of Millman, Winder & Griffiths[xxvi] (2017) show that many victims believe the police are not doing enough in matters like this while the police are of the opinion that online users should be more careful while engaging others via technology.

In the United States, several states have made attempts to address the twin challenge of cyber stalking and cyber harassment over the years. In addressing these problems, legislators have generally taken one of two approaches [xxvii](Fukuchi, 2011). In some states, legislators opted to amend or modify extant statutes prohibiting harassment or stalking, by adding language specifying that contact initiated using the Internet or other digital device would also constitute harassment or stalking. Statutes utilizing this first approach, therefore, do not have statutes specifically titled cyber harassment or cyber stalking, though acts constituting cyber harassment or cyber stalking are prohibited. The second approach, selected by some states, was to add new legislation explicitly defining and prohibiting cyber harassment or cyber stalking. In these states, there are separate statutes defining traditional, in person forms of harassment/stalking and cyber harassment or cyber stalking. The first state to do this was Connecticut. Michigan, Arizona and Virginia have also enacted similar legislation criminalising harassment by electronic means.[xxviii]

7. Legislative Framework against Cyber-Harassment in Nigeria

Section 24 of the Cybercrimes (Prohibition, Prevention Etc.) Act 2015 is actually titled 'Cyberstalking' and it provides as follows: "Any person who knowingly who knowingly or intentionally sends a message or other matter by means of computer systems or network that –

- Is grossly offensive, pornographic or of indecent, obscene or menacing character or causes any such message or matter to be so sent; or
- He knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another causes such message to be sent:
- Commits an offence under this act and shall be liable on conviction to a fine of not more than n7,000,000.00 or imprisonment for a term of not more than three years or to both such fine and imprisonment

Any person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network –

- to bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm to another person;
- containing any threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value; or
- Containing any threat to harm the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, to extort from any person, firm, association, or corporation, any money or other thing of value:

Commits an offence under this Act and shall be liable on conviction –

- In the case of paragraph (a) and (b) of this subsection to imprisonment for a term of 10 years and or a minimum fine of N25,000,000.00; and
- In the case of paragraph (c) and (d) of this subsection, to imprisonment for a term of 5 years and or a minimum fine of N15,000,000.00

A court sentencing or otherwise dealing with a person convicted of an offence under subsections (1) and (2) may also make an order, which may, for the purpose of protecting the victim or victims of the offence, or any other person mentioned in the order, from further conduct which –

- Amounts to harassment; or
- Will cause fear of violence, death or bodily harm; prohibit the defendant from doing anything described/specified in the order.

A defendant who does anything which he is prohibited from doing by an order under this section, commits an offence and shall be liable on conviction to a fine of not more than N10,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

The order made under subsection (3) of this section may have effect for a specified period or until further order and the defendant or any other person mentioned in the order may apply to the court which made the order for it to be varied or discharged by a further order.

Notwithstanding the powers of the court under subsections (3) and (5), the court may make an interim order for the protection of victim(s) from further exposure to the alleged offences.

The above provisions are novel and one must commend the legislature for the boldness to recognise this negative possibility via the internet. The inclusion of the medium of computer systems and computer network is a departure from the old Criminal Code Act which does not recognize such media because the law failed to catch up with the times.

A look at the provisions of the Cybercrime Act shows that the lawmakers were aware of the current possibilities via technology. The provisions of Section 24 clearly cover revenge porn, cyber bullying, cyber stalking and all forms of cyber harassment. It also goes to address wrongful use of electronic communication to extort money and sending of threats to kidnap another.

One of the beautiful provisions of the section is the power of the court under Section 24 (3) to prohibit further harassment in any form and this means a court can give a restraining order prohibiting an offender from any form of contact with the victim. The law empowers the court to impose a heavy fine of ten million naira or an imprisonment for a term of not more than three years on the offender who violates a court order earlier prohibiting him from further conduct amounting to harassment or any other conduct. Subsection (6) also empowers the court to make interim orders for the protection of the victim from the alleged offences.

This writer is of the opinion that the foregoing provisions are a right step in the right direction but more needs to be done to give reprieve to victims of this types of crimes. It is common knowledge that a larger part of Nigerian criminal laws attempts to serve as deterrents or stipulate outright punishment for convicted offenders. Not much has been done to consider the interest of the victims of criminal acts. This lack of remedies for the victims has discouraged many from reporting crimes. In a nation where public officers are reported to breach public trust with impunity and where justice sometimes seem to be beyond the reach of the poor, more need to be done to encourage victims to come forward.

8. Practical Solutions

Education is key to changing attitudes and making clear that the denigration of other people and violence against them are unacceptable. Apart from law enforcement agencies like the police, other relevant bodies like the Ministry of Information, the National Orientation Agency should take education of the populace to a more practical level. Education should not be limited to the classrooms and training institutions. The government should engage the electronic media and other means in changing people's attitudes towards others and making known the dangers in such practices.

Secondly, website owners and Internet Service Providers have definite roles in ensuring that improper content are not hosted on their websites or their servers. Facebook for example has definite policies of closing accounts that are reported for abuse. But recently, it went a step further when it announced that it would be relying on Artificial Intelligence to deal with revenge porn even before it is reported. Antigone Davis, the head of safety control at Facebook said the software would "proactively detect near nude images or videos that are shared without permission on Facebook and Instagram." The goal of this would be for Facebook to find and identify the content before the subject can report it, which would be tremendously helpful because "often victims are afraid of retribution so they are reluctant to report the content themselves, or are unaware the content has been shared," The image would then be reviewed by a (human) member of the Facebook team to confirm that it was posted without the subject's consent; if it was, the image would be removed, and the poster's account would be disabled.[xxix]

The foregoing example by Facebook speaks of the upward drive of technology and the need for the intermediaries to rise up to the challenges. Nigerian Internet service providers and website administrators must be more proactive against bullying and condescending speech and other traits that show lack of respect for the human dignity in cyberspace. Hiring moderators, banning users who abuse, bully, stalk or howsoever harass others, blocking anonymous users who perpetrate acts that are unbecoming of human conduct and sharing threats with authorities would be a great second step.

The third major step that should be taken is to train and retrain the police and other law enforcement agencies. Across the globe, many law enforcement departments are becoming internet savvy social media users. The Nigerian Police now has official pages on Twitter, Facebook and Instagram. These engagements on social media are welcome developments, but more than mere usage, officers also need to learn how to deal with cases of cyber-bullying and cyber-stalking. While efforts are made daily to deal with cyber-scams and all manners of internet fraud, there should be a sincere focus too on curbing electronic crime against persons.

Fourthly, perpetrators of cyber harassment should be arrested prosecuted and if found guilty, punished according to the provisions of the law. A slap on the wrist type of punishment will not stop perpetrators of cyber harassment from repeating the act especially when the victim is left without a remedy. It is possible that a serious jail term coupled with payment of a hefty fine will help potential internet trolls' reason and retrace their steps before publishing another online threat.

Fifthly, the Internet community in Nigeria must discuss these issues, and create clear and helpful guidelines for victims of online abuse. The government, though at the forefront cannot do everything required to curb these class of crimes. The silent danger in electronic crimes is the possibility of the planning and the execution from the comfort of a bedroom as long as the appropriate computer is available with internet access. The Internet community must do more than provide access and secure connectivity, awareness of the negative possibilities should be brought to the front view and suggestions and solutions found to these menaces.

None governmental organisations (NGOs) and Women and Children Rights Groups must step in to educate and support potential victims and outright victims of this class of crimes. This is one area where such bodies can be more impactful in protecting the vulnerable class as it is known that most victims of cyber stalking or cyber harassment are women and children. Further, in the age of technology, NGOs can take the lead to demand for more adequate legislation

that will not only deter potential offenders or punish the guilty ones but that will provide for adequate compensatory remedy for the victims. The place and roles of such groups cannot be over-emphasized in these matters.

9. Conclusions

We have tried to take a look at the legal framework for electronic crimes against persons in Nigeria. We have also observed that though the law has provisions preventing crimes against persons, the incidences made possible by technology have not been easy to handle like the physical ones. We also pointed out that the older legislations may not be adequate in many instances to deal with novel crimes because the older laws did not contemplate advances in technology and the more advanced nations have realised this and thus there is a drive for new legislations.

We made some attempt to examine the legislative provisions relating to cyber harassment in some jurisdictions and compared the same with Nigerian laws. We observed that while Nigerian lawmakers should be commended for enacting the Cybercrime Act, and especially the penalties stipulated therein, there is the need to make provision for compensation to victims of electronic crimes against person generally in Nigeria. We observed that generally, Nigeria has not responded to technological advancements by legislation as the advanced nations of the world have done. The paper concludes by suggesting practical solutions to help in the fight against cyber harassment in Nigeria.

10. References

i. Annese, J. A. (July 18, 2013). FBI: Stalker terrorized Harry Potter fan author, a former Staten Island Advance reporter, for years. Staten Island Advance. Retrieved from: http://www.silive.com/news/index.ssf/2013/07/fbi_stalker_terrorized_harry_p.html.
ii. Fukuchi, A. (2011). A Balance of Convenience: The Use of Burden-shifting Devices in Criminal Cyber harassment Law. Boston College Law Review, 52, 289-338.
iii. Garner, B. A., (ed) Black's Law Dictionary
iv. Goodno, N. H. (2007). CS, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws. Missouri Law Review, 72, 125-197.
v. Hazelwood, S. D. &Koon-Magnin, S., (2013) International Journal of Cyber Criminology Vol 7 Issue 2
vi. Kamal, A. (2005)The Law of Cyberspace – An Invitation to the Table of Negotiations 1st ed. United Nations Institute for Training and Research 2005, 55;
vii. Kamal, M., & Newman W. J., (2016) Revenge Pornography: Mental Health Implications and Related Legislation. Journal of the American Academy of Psychiatry and the Law 44 (3) 359-367
viii. Lanigan, R., "The Rise of Revenge Porn: Could Your Intimate Photos be splashed all over the Internet?" The Tab Belfast available at www.belfast.tab.co.uk/2014/04/17
ix. Millman, C., Winder, B. & Griffiths, M.D. (2017). UK-based police officers' perceptions of, and role in investigating, cyber-harassment as a crime. International Journal of Techno ethics, 8, 87- 102.
x. Paludi, M. A., (1991) Academic and Workplace Sexual Harassment. SUNY Press pp. 2-5
xi. Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyber-stalking victimization and offending among college students. Deviant Behavior, 33, 1- 25. doi: 10.1080/01639625.2010.538364

[i] Kamal, A.,(2005) The Law of Cyberspace – An Invitation to the Table of Negotiations 1st ed. United Nations Institute for Training and Research 2005, 55;

[ii] Revenge porn is defined as sexually explicit media that is publicly shared online without the consent of the pictured individual. See http://en.wikipedia.org/wiki/Revenge_porn accessed on 17th June 2014

[iii] The craze which started in America and has since spread to the UK, allows spurned ex-lovers to post their exes naked photographs, and worse real names, addresses and links to social media, all over the internet. See "The Rise of Revenge Porn: Could Your Intimate Photos be Splashed all over the Internet?" by Roisin Lanigan, The Tab Belfast available at www.belfast.tab.co.uk/2014/04/17

[iv] Welcome page of the Oxford Cyber Harassment Research Symposium available at www.cyber-harassment-research.org accessed on 19th July 2018

[v] Bryan A. Garner (ed) Blacks Law Dictionary

[vi] Stalking and Harassment: Legal Guidance: Crown Prosecution Service http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/#a05a assessed on 13th May 2014

[vii] Ibid

[viii] This is one of the identified causes of revenge porn which is discussed below.

[ix] Stalking and Harassment: Legal Guidance: Crown Prosecution Service http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/#a05a assessed on 13th May 2014

[x] The Convention on the Elimination of all Forms of Discrimination Against Women defines sexual harassment as including: such unwelcome sexually determined behavior as physical contact and advances, sexually colored remarks, showing pornography and sexual demands, whether by words or actions. Such conduct can be humiliating and may constitute a health and safety problem; it is discriminatory when the woman has reasonable ground to believe that her objection would disadvantage her in connection with her employment, including recruitment or promotion, or when it creates a hostile working environment.

[xi] Paludi, M. A., (1991) Academic and Workplace Sexual Harassment. SUNY Press pp. 2-5

[xii] "Bullying at Work" http://spunout.ie/life/article/bullying-at-work? Accessed on 17th June 2014

[xiii] Supra footnote 2 above

[xiv] Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyber-stalking victimization and offending among college students. Deviant behavior, 33, 1- 25. doi: 10.1080/01639625.2010.538364

[xv] Steven D. Hazelwood & Sarah Koon-Magnin (2013) International Journal of Cyber Criminology Vol 7 Issue 2

[xvi] Annese, J. A. (July 18, 2013). FBI: Stalker terrorized Harry Potter fan author, a former Staten Island Advance reporter, for years. Staten Island Advance. Retrieved from: http://www.silive.com/news/index.ssf/2013/07/fbi_stalker_terrorized_harry_p.html.

[xvii] Unreported, Suit No FHC/AD/17c/2017

[xviii] Kamal, M., & Newman W. J., (2016) Revenge Pornography: Mental Health Implications and Related Legislation. Journal of the American Academy of Psychiatry and the Law 44 (3) 359-367

[xix] "End Revenge Porn" A campaign of the Cyber Civil Rights Initiative https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf accessed on 9th May 2019
[xx]Cap 77 C39 Laws of the Federation of Nigeria 2004
[xxi]Section 2.
[xxii]These are contained in Part 5 of the Nigeria Criminal Code
[xxiii]See 'Offence against the Person' www.en.wikipedia.org/wiki/Offence_against_the_person assessed on 12th May 2014
[xxiv] Sections 373-381 of the Criminal Code
[xxv]Goodno, N. H. (2007). CS, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws. Missouri Law Review, 72, 125-197.
[xxvi]Millman, C., Winder, B. & Griffiths, M.D. (2017). UK-based Police Officers' Perceptions of, and Role in Investigating, Cyber-harassment as a Crime. International Journal of Technoethics, 8, 87- 102.
[xxvii]Fukuchi, A. (2011). A Balance of Convenience: The Use of Burden-shifting Devices in Criminal Cyberharassment Law. Boston College Law Review, 52, 289-338.
[xxviii]See for example Section 18.2-152.7:1, Code of Virginia. Legislative Information System of Virginia
[xxix]See "Facebook Says It's Putting an End to Revenge Porn Once and For All" RollingStone available at https://www.rollingstone.com/culture/culture-news/facebook-revenge-porn-ai-software-808867/ accessed on 9th May 2019