
CHILD & YOUTH PROTECTION FOUNDATION
LAYING A FOUNDATION FOR A GOOD FUTURE
R VISION
epresents the right of
uth; a society which
sitive and enabling
children and youth
d develop into
ible adults;
zed society
MISSION
THE CYBERCRIME ACT 2015
&
THE PROTECTION OF CHILDREN
IN NIGERIA
Type here to search
CHILD & YOUTH PROTECTION FOUNDATION
global fund for children
Girl to Woman
PRISTINE CONCEPTS

INTRODUCTION

In today's world Nigeria inclusive, information technology enhances almost every facet of our daily lives as through the internet and computers we are able to connect and transact businesses across borders and physical territories with huge amounts of data been stored, processed and retrieved. The Internet has also brought untold benefits to children around the world as it creates unprecedented opportunities to connect, share, learn, access information cementing their place and identity in online communities.

However, the Internet has raised new and disturbing issues of vulnerability, especially where children are concerned with growing attention on the distribution of abuse materials targeted at children, making them vulnerable to different variety of cybercrimes ranging from, cyber bullying, texting/sexting, dangers of sexual solicitation, exposure to problematic /illegal content and privacy violations. It then becomes necessary to explore the legal protections in place that safeguards them from such acts and combat same in the event they occur.

What is Cybercrime

Cybercrime encompasses all forms of cyber assisted criminal activity in which its commission is partly or totally aided by cyber space and/or its components usually committed through a computer which could be the object of the crime or a tool to commit an offense. It encompasses a wide range of activities, but these can generally be broken into two categories:

- Crimes that target computer networks or devices which includes viruses and denial-of-service attacks.
- Crimes that use computer networks to advance other criminal activities which includes cyber stalking, phishing and fraud or identity theft.

Those who commit cybercrime are known as cyber criminals or cyber crooks. As this type of crime can be committed from a distant location; for example-a foreign country, most criminals prefer this mode as the risk of getting traced and punished is limited.

Who is a CHILD ?

A child under the Child Rights Act is a person under the age of eighteen years. Similar the United Nations Convention on the Rights of the Child (UNCRC) defines the child as a person under 18 years of age. It acknowledges the primary role of parents and the family in the care and protection of children, as well as the obligation of the State to help them carry out these duties.

The Cybercrimes Prohibition, Prevention etc. Act, 2015 (The Act)

The Cybercrimes Act is the first legislation in Nigeria that deals specifically with cyber security, passed in May 2015, it gives effect to the 2011 ECOWAS Directive on fighting cybercrime. It is an act to provide for the prohibition, prevention, detection, response, investigation and prosecution of cybercrimes. It also ensures the protection of critical national information infrastructure promotes cyber security, protects computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

CYPF LAYING A FOUNDATION FOR A GOOD FUTURE
CHILD & YOUTH PROTECTION FOUNDATION
global fund for children
Girl to Woman
PRISTINE CONCEPTS

Importance of Child Protection against Cybercrimes

The importance of protecting children against cybercrimes cannot be overemphasized as technological innovations simultaneously have allowed violence to be committed by, with, and through the use of ICTs. Children are particularly vulnerable to the exploitation of online predators because they rely heavily on networking websites for social interaction. Offenders use false identities in chat rooms to lure victims into physical meetings, thus connecting the worlds of cyber and physical crime. When this happens, virtual crime often leads to traditional forms of child abuse and exploitation such as trafficking and sex tourism. Furthermore exposure to harmful online content may cause direct harm to the child (as viewer of the material) and indirect harm to children because sex offenders can use the Internet and associated technologies to expose them to sexually exploitative materials which might normalize such sexual activities.

In addition, victims of online exploitation must live with their abuse for the rest of their lives because once such information and images are online, they remain there forever and are available to an increasing number of persons which in turn has psychological effects on the victims.

Thus it becomes necessary that there are effective laws that exist to protect children from online abuse and exploitation and efficient implementation mechanisms in place to prevent and deal with such acts in the event it occurs.

Provisions relating To Child Protection / Interpretations in the Act

There are different crimes relating to/protection accorded to children which are provided for under the Act and they include;

Child Pornography

According to the Act, child pornography shall include pornographic material that visually depicts:

- a minor engaged in sexually explicit conduct;
- a person appearing to be a minor engaged in sexually explicit conduct; and
- realistic images representing a minor engaged in sexually explicit conduct.

In this aspect, there are different categories of offences provided under the Act which are all punishable and they are:

Creation and Transmission of Child Pornography

These acts usually include the making, dissemination, storage, circulation, publication and transmission of information containing child pornography or child sexual exploitation in electronic form. Damages resulting from such acts can cause harm to children especially as it would be difficult to restore children's rights once information harmful to the interests of children circulates on the Internet.

Thus the Act provides that any person who intentionally uses any computer system or network in or for such an act would be liable on imprisonment for a term of 10 years or a fine of not more than N20 milli

Unsolicited Distribution of Child Pornographic Images

This involves the sharing or sending of images that contain pornographic content among a number of persons or groups without consent from the recipients. Thus this could include sharing and sending of such images on social media platforms like Whatsapp, Facebook and similar networks. In trying to protect against such, the Act provides that any person who knowingly makes or sends other pornographic images to another computer by way of unsolicited distribution shall upon conviction be sentenced to One year imprisonment or a fine of N250 thousand or both.

Procurement and Possession of Child Pornography

Child pornography possession is an unusual sex crime as it is a form of child sexual exploitation that requires no direct interaction with a victim. It involves receiving and keeping images that are contraband because they show actual children (often unidentified) being sexually abused and exploited. Although a sexual motive is not required for the crime, having Child Pornography certainly suggests such a motive, and there is evidence that many perpetrators of such are sexually interested in children. Thus the Act provides that any person who procures child pornography for oneself or for another person, possesses child pornography in a computer system or on a computer-data storage medium shall be liable on conviction to imprisonment for a term of not more than 5 years or a fine of not more than N10 million or to both.

Online Sexual Solicitation of Children, Grooming, Luring or Predation

This is a situation where minors are engaged in sexually orientated communications (e.g., "computer chat") often with the intention of arranging offline sexual encounters. This communication is frequently on-going and a relationship between the offender and target can develop over the course of several weeks or months and can contain very explicit sexual content. Thus in furtherance of this, the Act provides that any person who, intentionally engages in such activities with a child would be liable on conviction to imprisonment for a term of not more than 10 years and a fine of not more than N15 million.

Furthermore where such sexual solicitation is made

- Under coercion, inducement, force or threats;
- By a person in a recognized position of trust, authority or influence over the child, including within the family;
- Of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence;
- By recruiting, inducing, coercing, exposing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child;

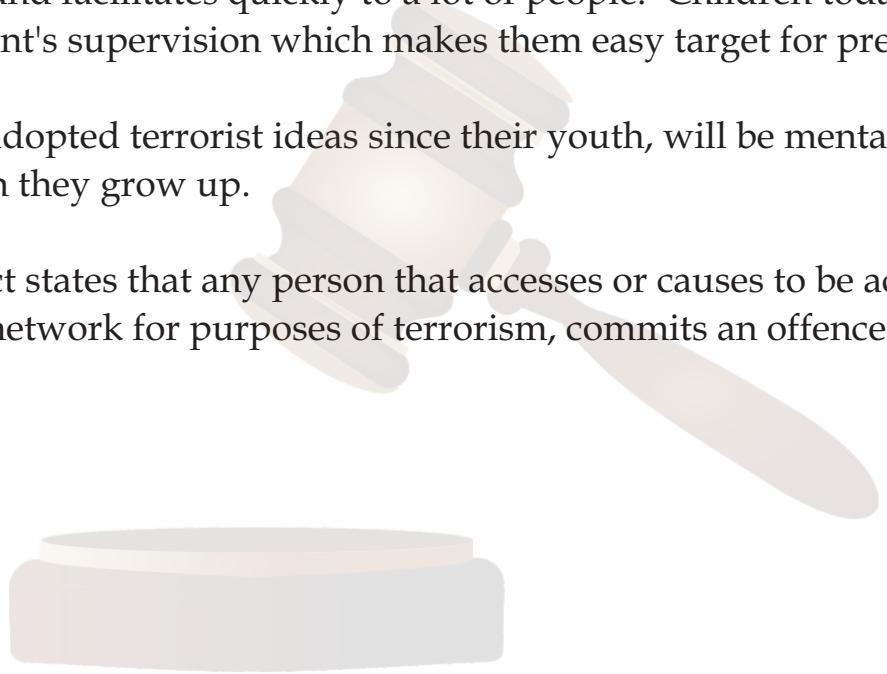
Such person shall upon conviction be liable to imprisonment for a term of not more than 15 years and a fine of not more than N25 million.

Cyber Terrorism

Cyber terrorism is the use of the internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. Due to the convenience, affordability, and broad reach of social media platforms such as Youtube, Facebook and Twitter, terrorist groups and individuals have increasingly used social media to further their goals, recruit members, and spread their message. They resort to this medium because it's cheap, accessible and facilitates quickly to a lot of people. Children today spend more time on the Internet without parent's supervision which makes them easy target for presenting radical ideas and materials.

Children, who have adopted terrorist ideas since their youth, will be mentally prepared to conduct any terrorist act when they grow up.

In light of this, the Act states that any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.



Cyber bullying or Harassment

Cyber-bullying is described as the use of information and communication technology, for the harassment or mistreatment of another. It includes sending, posting, or sharing negative, harmful, false, or mean content about someone else causing embarrassment or humiliation. Severe, long-term, or frequent cyber bullying can leave both victims and bullies at greater risk for anxiety, depression, and other stress-related disorders as they also become easy targets for adult harassers who may exploit them sexually and in some rare but highly publicized cases, some children have turned to suicide.

In view of this, the Act provides that 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 or to another person shall be liable on conviction to imprisonment for a term of 10 years and/or a minimum fine of N25 million.
- 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 and shall be liable on conviction to imprisonment for a term of 5 yearsand/or a minimum fine of N15 million.

Data Retention /Preservation/ Privacy Provisions

Data usually includes subscriber information (i.e., data that helps identify the subscriber), as well as traffic data (i.e., information on the route, time, date, duration, destination, and source of a communication). Thus insufficient provision for the retention and preservation of non-content based data is a significant barrier to identifying and locating suspects and criminal prosecutions in ICT-facilitated offenses against children. Thus the Act requires service providers to keep all traffic data and subscriber information for a period of two years. However such data shall not be utilized except for legitimate purposes provided for under the Act, any other legislation, regulation or by an order of a court of competent jurisdiction. Furthermore in order to ensure the data of children are safeguarded, it provides that due regard shall be had to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and appropriate measures shall be taken to safeguard the Confidentiality of the data retained, processed or retrieved for the purpose of law enforcement. Anyone who contravenes these provisions shall be liable on conviction to a term not exceeding 3 years or a fine not more than 7 million naira or both.

Interception of Communication

Due to the fact the Cybercrimes are committed mostly through the internet which affords anonymity, it becomes important that in order to prosecute crimes against children that such communications should be intercepted and this includes listening to the calls made on a telephone or opening and reading the contents of a target's letters or e-mails or chats. Thus the Act allows for the interception of electronic communication, by way of a court order by a Judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings or authorization of a law enforcement officer to collect or record same.

Creation of the Cybercrime Advisory Council

The Act also created the Cybercrime Advisory Council which is responsible for policy formulation, while the Office of the National Security Adviser (ONSA) is responsible for the enforcement of the Act.[3] The council has the power to advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues which would of course be extended to the protection of children.

Racist/ Xenophobic Comments

These includes any material(written or printed), any image or any other representation of ideas or theories which promotes or incites hatred, discrimination or violence against any individual based on race, color, descent, national or ethnic origin as well as religion if used as a pretext for any of these factors. In furtherance of this, the Act provides that any person who intentionally distributes or makes available such materials to the public or threatens or insults persons with such racists and xenophobic comments shall on conviction be liable to not more than 5 years imprisonment or a fine not more than 10 million or both.

Attempt, Conspiracy, Aiding and Abetting

it is important to know that any person, who attempts to commit any of the offences already mentioned or aids, abets, conspires, counsels or procures another person(s) to commit any of such acts commits an offence and shall be liable on conviction to the punishment provided for the principal offence under the Act.

Challenges with Enforcement of the Cybercrimes Act

- It is important to note that the Cyber crimes Act was drafted long before being signed into law in 2015 and considering the rapid rate at which technology develops, the manner cyber criminals continue to outpace legal developments and the different forms of cyber related offences that keeps evolving, the Act presently may no longer be able to keep up with the trends of cyber environment. For example the Act fails to make provisions for different forms of cyber bullying and does not have provisions criminalizing advertised child sex tourism through the Internet and associated technologies

- Cybercrime is global as victims can be located in one country, while the perpetrators are in another. Thus it becomes easy to have and locate victims in Nigeria while the persons who committed such crimes may be in other countries making it difficult for law enforcement to locate and prosecute them.

- For many, the internet is about freedom and uninhibited creativity, thus Criminal enterprises benefit from the relative anonymity the internet provides and as such Law enforcement authorities struggle to locate offenders because of the ability to conceal online identities and shield unlawful activities with security programs. Furthermore many Internet cafés also afford anonymity, without requiring the identification of their users to log on to computers.

Though the Act enjoins Cybercafés to maintain registers of users through a sign in register which shall be available to law enforcement personnel whenever needed, most cybercafés do not implement this process and are never supervised or inspected to ensure compliance with this provision.
This in turn makes it difficult for perpetrators to be caught.

- Families and communities as parents and legal guardians are supposed to be the first line of protection for children by supervising and monitoring them while they use the internet. However, they are usually too busy, do not care or treat their children with laxity when they access the internet. When these categories of persons become unaware of when their children are been exploited, it then becomes impossible to prevent, report or prosecute such offenders.
Furthermore, many Nigerians fail to report child exploitation cases online leaving the perpetrators to run free and carry on such acts on other children. This could be as a result to lack of enlightenment on the Act, ignorance or failure to attach much importance to such acts.
This also poses a huge problem when it comes to the enforcement of the provisions of the Act.

- The Act fails to give proper attention to cyber bullying as the provisions of the Act only extend to cyber-stalking, racist and xenophobic remarks. The wording on these two provisions is not sufficient to cover the various forms of cyber-bullying existing in the world today such as mockery, trolling, dissing, masquerading, trickery among others which need not be false, offensive or incite fear of death. Furthermore the average Nigerian downplays cyber bullying believing it isn't a Nigerian thing which could be attributed to the fact that it does not involve physical contact. Thus much attention isn't put on this form of crime making the enforcement and prosecution difficult.

- The Act is commendable as it makes provisions for these offences but as it is with Nigerian laws, the issue of enforcement still remains a big issue. Cybercrime offences against children aren't given enough attention so the prosecution of cases in this area isn't vibrant and agencies charged with enforcing the provisions of the Act are not active.
Thus the provisions of the Act remain in a comatose state.

Recommendations

- Traditional methods of solving crimes have become unhelpful with the computerization of these crimes thus Agencies in the prosecution of cyber crimes should be educated on how to tackle the recent development in the internet with the goal being to better understand the scope of cyber crime and the nature of the criminal enterprise while recognizing that the tactics of cyber criminals will evolve as preventative and punitive measures develop.

- Though there exists provisions in the Act to prevent the use of public computers in cybercafés for criminal purposes, there should exist further provisions that enjoins intended users of a cybercafés to provide documents identifying themselves while records of such document be kept by storing either a photocopy or a scanned copy of the document duly authenticated by the user and an authorized representative of the cybercafé. Furthermore follow up actions by agencies should be carried out to ensure the enforcement of the provision.

- Parents and guardians also have a prominent role to play in prevention of cybercrimes as the law cannot work in isolation when it comes to matters relating to children. Thus persons in such roles should ensure they monitor the use of their child's online activity and report suspicious behavior, websites hosting exploitative images and efforts to recruit or groom children for sexual abuse.

- Domestic awareness campaigns should be carried out by the relevant agencies on the causes and legal consequences of cyber crimes on children which should be targeted to children, parents, and educators and such campaigns should include necessary information to protect and prevent against online predators.

- Professionals who, in their everyday, professional capacity, come into contact with children and owe them certain duty of care should also be required to report suspected child pornography activities and/or child pornography offenses to law enforcement or another agency. Financial institutions (i.e. credit card companies, banks) as well should be mandated to report same, once they become aware of such circumstances, considering that payment services rendered by such organizations or corporations are being used to proliferate child pornography.

- Though Nigeria does not attribute much importance to bullying more so cyber bullying but its occurrence among children cannot be denied. Thus in combatting this, establishers of Schools as well as the school should conduct necessary awareness activities for children enrolled in their Institutions and their custodians (or parents) for the prevention and effective handling of bullying committed through the Internet. The Act should also provide effective means of prosecuting cases of cyber bullying and creating effective awareness in respect of the Cyber crimes Act in order to encourage victims of cyber bullying to document such acts and report the offenders.

- It is important that Nigeria enacts a Child Online Protection Act and a Child Privacy Protection Act so that such provisions would sufficiently provide for the protection of children from online activities that may be harmful to them. The Act could also make provisions that limit the liability of ISPs, as long as they remove child pornography and take measures to prevent the further transmission of such content when they learn of its presence on their own networks. Such Acts should also create agencies that would specifically enforce the provisions of the Act and should have the mandate to conduct investigations and act on complaints.

CONCLUSION

In view of the fact that ICT is rapidly taking over the world, the rate at which children have access to the internet and the fact that violence is been committed by, with and through the internet, the cyberspace is no longer a safe environment. This brings us to why the cybercrime Act is extremely relevant as it provides for several offences that protects children from abuse and punishes offenders of those crimes. However whenit comes to children, laws can't work alone thus it becomes important that the society which includes parents, teachers, guardians, caretakers and the likes work in tandem with the law by monitoring and counseling children, reporting abuses among others so that we create a safe environment where children can access the internet free from all forms of abuse

Barrister Husseina Shaibu
Legal Officer,
CHILD AND YOUTH PROTECTION FOUNDATION

APPENDIX I.

1.Anita Persisin 'Alqaeda online Radicalization and the creation of Children Terrorists' (2014) <https://hrcak.srce.hr/file/186773> accessed 3/11/2019.

2. Children's Right Alliance 'The United Nations Convention on the Rights of the Child'<https://childrensrights.ie/childrens-rights-ireland/un-convention-rights-child> accessed 25/10/2019.

3.Flutterwave 'Cyberbullying: A Nigerian Perspective' (2019) <https://flutterwave.com/ng/blog/inside-flutterwave/cyber-bullying-a-nigerian-perspective/> accessed 5/10/2019.

4.Larrisa Hirsch 'Cyberbullying' (2014) <https://kidshealth.org/en/parents/cyberbullying.html> accessed 5/10/2019.

5.James Okoh and Enyinnaya Danjuma Chukwueke 'The Nigerian Cybercrime Act 2015 and Its Implications for Financial Institutions and Service Providers' (2016) <https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its-implications-for-financial-institutions-and-service-providers#.XX-V_FxKjIU> accessed 3/11/2019.

6.Janis Wolak and David Finkelhor and Kimberly Mitchell 'Child Pornography Possessors: Trends in Offender and Case Characteristics' (2011) *Journal on Research and Treatment* <http://unh.edu/ccrc/pdf/CV204%20CP%20possessors.pdf> accessed 1/10/2019

7.Oluwafemi Osha, 'National Policy and Strategy of Nigeria A qualitative Analysis' (2015) 9(1) *International Journal of Cyber Criminology* <https://www.researchgate.net/publication/282026229_National_Policy_and_Strategy_of_Nigeria_A_Qualitative_Analysis> accessed 7/10/2019.

8.Report of the World Bank and The International Center for Missing Persons and Exploited Children 'Protection Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming and Cyberbullying' (2015) <https://www.icmec.org/wp-content/uploads/2015/10/Protecting_Children_from_Cybercrime_-_Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf> accessed 1/11/2019.

9.Reve Antivirus 'Cybercrimes' (2019) < https://www.reveantivirus.com/en/computer-security-threats/cybercrime>, accessed 7/10 2019.

APPENDIX II.

10.Stopbullying.gov 'What is Cyber bullying' (2019) <https://www.stopbullying.gov/cyberbullying/what-is-it/index.html> accessed 2019.
11.Techopedia 'Cybercrime' (2019) <https://www.techopedia.com/definition/2387/cybercrime> Accessed 1/10/2019.
12.The Childs Right Act no 26 of 2003.
13.The Cybercrimes (Prohibition, Prevention etc.) Act of 2015.
14.The United Nations Convention of the Rights of the Child of 1989.
15.United Nations Office on Drugs and Crime 'Cybercrime: Protecting Children from Online Abuse and Exploitation' (2015) <https://www.unodc.org/unodc/en/frontpage/2015/July/cybercrime_-protecting-children-from-online-abuse-and-exploitation.html> accessed 3/11/2019..
16.Wikipedia 'Terrorism and Social Media' (2019) <https://en.wikipedia.org/wiki/Terrorism_and_social_media> accessed 11/10/ 2019.
17.United Nations Office on Drugs and Crime 'Cybercrime: Protecting Children from Online Abuse and Exploitation' (2015) <https://www.unodc.org/unodc/en/frontpage/2015/July/cybercrime_-protecting-children-from-online-abuse-and-exploitation.html> accessed 3/11/2019.

CHILD & YOUTH PROTECTION FOUNDATION

global fund for children

Girl to Woman

PRISTINE CONCEPTS