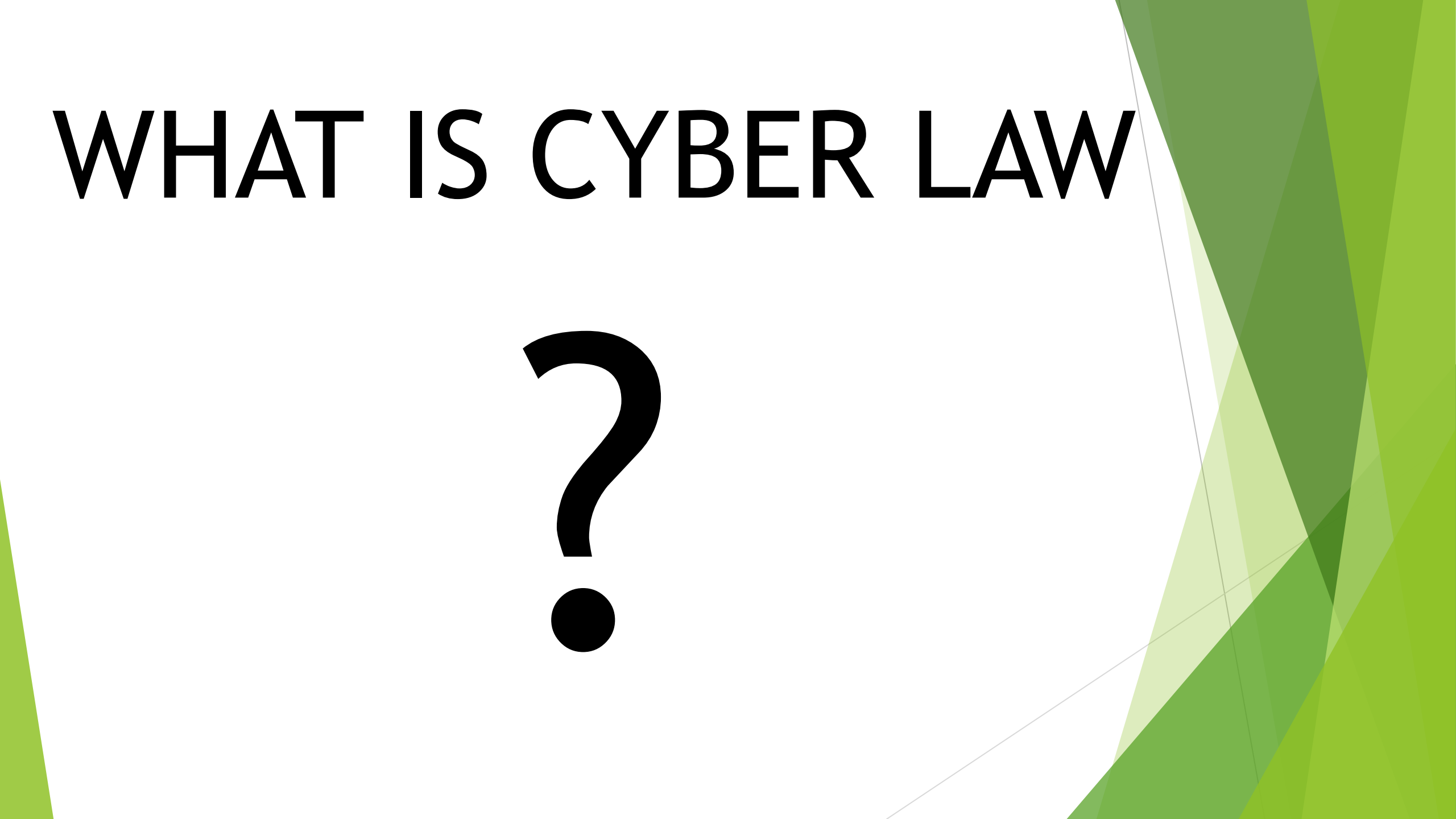
LEGAL FRAMEWORK FOR THE ENFORCEMENT OF CYBER LAW AND CYBER ETHICS IN NIGERIA

Umejiaku Nneka Obiamaka, Department of Commercial and Property Law

Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria

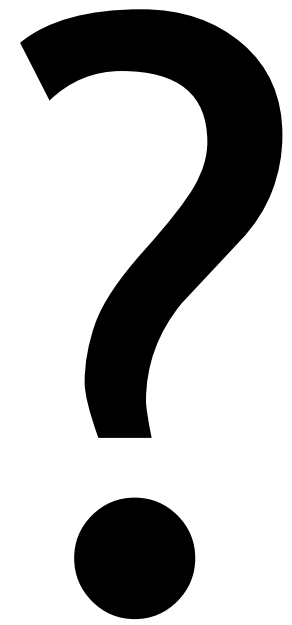
E-mail:nnekaumejiaku@gmail.com

WHAT IS CYBER LAW



Cyber law deals with codified rules and principles that regulate the activities of internet users. These rules/principles govern the exchange of communication and information for the protection of intellectual property, rights of freedom of speech and public access to information in cyber space.

WHAT IS CYBER ETHICS



Cyber Ethics is simply the responsible behaviour in the internet. It is the philosophical study of ethics pertaining to computers, encompassing user behaviour, and what computers are programmed to do and how it affects individuals and society.

Differences Between CYBER law & Ethics

CYBER LAW

- Laws are formal written directives that apply to everyone.
- It is interpreted by the judicial system and enforced by state,
- Laws have penalties associated with it.

CYBER ETHICS

- Ethics generally is the study of what is good for both the individual and the society.
- It is a moral obligation or duty one owes another
- It also refers to standard of character, set up by any race or nation
- Ethics don’t have penalties associated with it.

Regulation of Internet or The Cyberspace.

There are different opinion on the regulation of the cyber space for instance some aver that the internet should be regulated while some aver that it should not by preferring the following reasons.

1. The internet is global in nature and therefore should not be regulated.
2. The internet is not like other electronic media and therefore should not be regulated.
3. The government should not interfere with what children watch and do in the internet.

Cyber crime Act 2015

- The cybercrime Act is made up of 59 section, 8 part and 2 schedules. 1st schedule lists the cyber crime Advisory council while the 2nd schedule list businesses to be levied for the purpose of the cyber security fund.

Under section 44 (2) (a)GSM service providers and all telecom companies internet service providers: Bankers and other financial institutions insurance companies and Nigeria stock exchanges.

- The principles around cyber crime legislations require that the law focuses on computer-related offences content-related offences and computer integrity offences, jurisdiction and procedural issues-but a review of the law indicates that in addition to meeting the foregoing milestones, the drafters made strenuous efforts in seeking to bank transaction that is not the major focus of the Act

- The Act generally provides for punishment for every crime committed in the internet.
- The objective of the Act is for the unified legal regulatory framework for the prohibition, prevention, detection, prosecution and punishment of the cybercrimes in Nigeria.
- The Act defines the liabilities of service providers and ensures that national interest is not compromised by the electronic communication and transaction between public and private bodies
- The Act empowers the president to designate certain computer system networks and information infrastructure and to implement procedures ,guidelines and conduct audits for the furtherance of that.
- 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

Types of Crimes Provided/Protected by The Act

- Cyber stalking: Incudes intentionally sending of mails computer system that is grossly offensive or pornographic. It also include message that will annoy, endeavour, inconvenience insult and cause criminal intimidation to another person in fear of death, violence or bodily harm.
- Cyber squatting: This involves intentional use of a name, business name, trademark domain name or other word or phrase registered, aimed or in use by any individual body corporate or belonging to either the Federal State or Local Government in Nigeria on the Internet or any other computer network without authority or right and for the purpose of interfer with their use by the owner.
- Manipulation of ATM: The Act provides that any person who manipulates an ATM machine or point of sale terminal with the intention to defraud shall be guilty of an offence and upon conviction sentenced to five years imprisonment.
- Phishing/Spamming: The Act provides that any person who intentionally engages in computer phishing shall be liable upon conviction to three years imprisonment or a prime.
- Spreading of Computer Virus: The Act provides that anyone who engages in malicious or deliberate spread of viruses or any malware that causes damage to critical information in public or private or financial institution computer shall be guilty .

The Act also made elaborate provisions in its quest to protect Nigeria from unscrupulous elements.

1999 Constitution (as amended)

- The constitution is the first point of call for the regulation of the internet under the Nigerian legal jurisprudence. Section 37 provides for the rights of privacy.
- This rights extends to their homes correspondence, telephone conversation and telegraphic communication.

The Economic and Financial Crime Commission Act, 2004

- This Act provides the legal framework for investigation of all financial crimes including advance free fraud ,money laundering, charge transfers ,fraudulent encashment of negotiable instrument ,computer credit card fraud ,contract scam among others.
- Apart from cybercrime Act 2015.the Economic and Financial Crime is the only law in Nigeria that deals with internet service providers and cyber café, it does not deal with the broad spectrum of computers misuse and cybercrime as cited by the criminal code.

Criminal Code ACT 1990

- The criminal code criminalizes any type of stealing of funds in whatever form under this Act. Although cybercrime is not mentioned in the Act
- Sec419 specifically provides for obtaining property by false pretences or cheating. It states that any person who by any false pretence and with intent to defraud obtains from any other person anything capable of being stolen is guilty of a felony and is liable to imprisonment for three years.

Factors that Exacerbate Cyber Crime In Nigeria.

- The following factors exacerbate cybercrime in Nigeria.
- Jurisdiction
- Lack of implementation
- Lack or adequate monitoring
- Poor monitoring and non-regulation
- Porous nature of the internet
- Increase dependency on the internet
- Imperfection of domestic legislation
- Absence of international Legal framework

Conclusion

- The recent increase in cybercrime is a major concern to the world especially with regards to e-commerce.
- To manoeuvre the activities of cyber criminals law must be combined with ethics to curb the menace of cyber crimes.
- Apart from law and ethics international legal framework must be put in place to properly address the issue of cyber crime.

Recommendation

- Adequate Legislation and implementation
- Continuous education
- Creation of awareness
- Making viable laws to control the activities of cyber criminals
- Legislating international frame works to combat the menace of cyber crimes.