CST812: CYBER LAW

AFRICA CENTRE OF EXCELLENCE ON TECHNOLOGY ENHANCED LEARNING (ACETEL)

NATIONAL OPEN UNIVERSITY OF NIGERIA

Course Guide for CST812

Introduction

CST812 – Cyber Law and Ethics is a 2-credit unit. The course is a compulsory course in second semester. It will take you 15 weeks to complete the course. You are to spend 65 hours of study for a period of 13 weeks while the first week is for orientation and the last week is for end of semester examination.

You will receive the course material which you can read online or download and read off-line. The online course material is integrated in the Learning Management System (LMS). All activities in this course will be held in the LMS. All you need to know in this course is presented in the following sub-headings.

Course Competencies

By the end of this course, you will gain competency to:

- Apply the laws guiding the use of cyberspace

Course Objectives

The course objectives are to:

- Analyze statutory, regulatory, constitutional, and organizational laws as it is applied to cybersecurity
- Explore the laws of other countries in relation to cyberspace
- Demonstrate the ethical issues surrounding the use of the internet

Working Through this Course

The course is divided into modules and units. The modules are derived from the course competencies and objectives. The competencies will guide you on the skills you will gain at the end of this course. So, as you work through the course, reflect on the competencies to ensure mastery. The units are components of the modules. Each unit is sub-divided into introduction, intended learning outcome(s), main content, self-assessment exercise(s), conclusion, summary, and further readings. The introduction introduces you to the unit topic. The intended learning outcome(s) is the central point which help to measure your achievement or success in the course. Therefore, study the intended learning outcome(s) before going to the main content and at the

end of the unit, revisit the intended learning outcome(s) to check if you have achieved the learning outcomes. Work through the unit again if you have not attained the stated learning outcomes.

The main content is the body of knowledge in the unit. Self-assessment exercises are embedded in the content which helps you to evaluate your mastery of the competencies. The conclusion gives you the takeaway while the summary is a brief of the knowledge presented in the unit. The final part is the further readings. This takes you to where you can read more on the knowledge or topic presented in the unit. The modules and units are presented as follows:

Module 1 The Internet

Unit 1 Legal Framework of cyberspace
Unit 2 Privacy and Censorship
Unit 3 Net Neutrality

Module 2 Cyber law in Nigeria

Unit 1 Advance Fee Fraud and Other Fraud Related Offences (Amendment) Act
Unit 2 Cybercrime Act
Unit 3 Evidence Act
Unit 4 Nigeria Data Protection Regulation, cybercrime policy and strategy

Module 3 Cyber Law: International Perspective

Unit 1 UN & International Telecommunication Union (ITU) Initiative
Unit 2 Council of Europe-Budapest Convention on Cybercrime

Module 4 Dispute in Cyberspace

Unit 1 Intellectual Property Issues
Unit 2 Jurisdiction and International law

Module 5 Cyber Ethics and Emerging Trends

Unit 1 Ethical Concepts and Professionalism
Unit 2 Emerging Trends in Cyber Laws and Ethics

There are thirteen units in this course. Each unit represent a week of study.

Presentation Schedule

The weekly activities are presented in Table 1 while the required hours of study and the activities are presented in Table 2. This will guide your study time. You may spend more time in completing each module or unit.

Table I: Weekly Activities

Week	Activity
1	Orientation and course guide
2	Module 1 Unit 1
3	Module 1 Unit 2
4	Module 1 Unit 3
5	Module 2 Unit 1
6	Module 2 Unit 2
7	Module 2 Unit 3
8	Module 2 Unit 4
9	Module 3 Unit 1
10	Module 3 Unit 2
11	Module 4 Units 1 and 2
12	Module 5 Unit 1
13	Module 5 Unit 2
14	Revision and Response to Questionnaire
15	Examination

The activities in Table I include facilitation hours (synchronous and asynchronous), assignments, mini projects, and laboratory practical. How do you know the hours to spend on each? A guide is presented in Table 2.

Table 2: Required Minimum Hours of Study

S/N	Activity	Hour per Week	Hour per Semester
1	Synchronous Facilitation (Video Conferencing)	1	13
2	Asynchronous Facilitation (Read and respond to posts including facilitator's comment, self-study)	3	39
3	Assignments, mini-project, laboratory practical and portfolios	1	13
	Total	5	65

Assessment

Table 3 presents the mode you will be assessed.

Table 3: Assessment

S/N	Method of Assessment	Score (%)
1	Portfolios	10
2	Mini Projects with presentation	20
3	Laboratory Practical	20
4	Assignments	10
5	Final Examination	40
Total		100

Portfolio

A portfolio has been created for you tagged "**My Portfolio**". With the use of Microsoft Word, state the knowledge you gained in every Module and in not more than three sentences explain how you were able to apply the knowledge to solve problems or challenges in your context or how you intend to apply the knowledge. Use this Table format:

Application of Knowledge Gained

Module	Topic	Knowledge Gained	Application of Knowledge Gained

You may be required to present your portfolio to a constituted panel.

Mini Projects with presentation

You are to work on the project according to specification. You may be required to defend your project. You will receive feedback on your project defence or after scoring. This project is different from your thesis.

Laboratory Practical

The laboratory practical may be virtual or face-to-face or both depending on the nature of the activity. You will receive further guidance from your facilitator.

Assignments

Take the assignment and click on the submission button to submit. The assignment will be scored, and you will receive a feedback.

Examination

Finally, the examination will help to test the cognitive domain. The test items will be mostly application, and evaluation test items that will lead to creation of new knowledge/idea.

How to get the Most from the Course

To get the most in this course, you:

- Need a personal laptop. The use of mobile phone only may not give you the desirable environment to work.
- Need regular and stable internet.
- Need to install the recommended software.
- Must work through the course step by step starting with the programme orientation.
- Must not plagiarise or impersonate. These are serious offences that could terminate your studentship. Plagiarism check will be used to run all your submissions.
- Must do all the assessments following given instructions.
- Must create time daily to attend to your study.

Facilitation

There will be two forms of facilitation – synchronous and asynchronous. The synchronous will be held through video conferencing according to weekly schedule. During the synchronous facilitation:

- There will be one hour of online real time contact per week making a total of 13 hours for thirteen weeks of study time.

- At the end of each video conferencing, the video will be uploaded for view at your pace.
- You are to read the course material and do other assignments as may be given before video conferencing time.
- The facilitator will concentrate on main themes.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

For the asynchronous facilitation, your facilitator will:

- Present the theme for the week.
- Direct and summarise forum discussions.
- Coordinate activities in the platform.
- Score and grade activities when need be.
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures, and podcasts if need be.

Read all the comments and notes of your facilitator especially on your assignments, participate in forum discussions. This will give you opportunity to socialise with others in the course and build your skill for teamwork. You can raise any challenge encountered during your study. To gain the maximum benefit from course facilitation, prepare a list of questions before the synchronous session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help ACETEL to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

Learner Support

You will receive the following support:

- Technical Support: There will be contact number(s), email address and chatbot on the Learning Management System where you can chat or send message to get assistance and guidance any time during the course.

- 24/7 communication: You can send personal mail to your facilitator and the centre at any time of the day. You will receive answer to you mails within 24 hours. There is also opportunity for personal or group chats at any time of the day with those that are online.

- You will receive guidance and feedback on your assessments, academic progress, and receive help to resolve challenges facing your stuides.

Course Information

Course Code:	CST 812
Course Title:	Cyber Law and Ethics
Credit Unit:	2
Course Status:	Compulsory
Course Blub:	In this course, you will learn about the legal and policy challenges of evolving cybersecurity threats at the national and international level, legal frameworks; cyber regulation, standards, law, and technology; national and international governing authorities; security governance and policy; privacy law; security policy development cycle; property-rights legislation; virtue ethics; utilitarian ethics and deontological ethics.
Semester:	Second
Course Duration:	13 weeks
Required Hours for Study:	65

Course Team

Course Developer:	ACETEL
Course Writers:	Dr Umar Suleiman Dauda and Dr Ibrahim A. Lawal
Content Editor:	Dr Ismaila Idris
Instructional Designers:	Inegbedion, Juliet O. (PhD) and Dr Lukuman Bello
Learning Technologists:	Dr Adewale Adesina and Mr Miracle David
Graphic Artist:	Mr Henry Udeh
Proofreader:	Mr Awe Olaniyan Joseph

Module 1: The Internet

Module Introduction

Welcome to the Internet module. This module will be completed within 10 hours; it will be supported with videos and exercises that will allow you to learn the most important concepts of the Internet. The module is the first one in the course sets out to present the legal framework of cyberspace. You will also easily learn about privacy and censorship. Finally, you will also learn then net Neutrality.

Introduction to the Internet

The Internet is an interconnection of different networks around the world. It is a broad public repository where files and services are exchanged reciprocally. The Internet is a distributed web of interconnected computer networks that support trillions of users worldwide using the standard Internet Protocol Suite (TCP / IP). It is a network of networks made up of millions of private, public, academic, business , and government networks ranging from local to global, connected through a wide array of electronic, wireless, and optical networking technologies..

Students and educational purposes usually use the internet to gather knowledge to do the study or to raise understanding of different subjects. Professionals from the industry and specialists including physicians also have access to the internet to find the information they need for their use. Hence the internet is for everyone the largest website in all age groups. The number of resources offered by the Internet is massive, ranging from simple home requirements to satisfying global corporate needs. It is used by people of all ages, by people from various countries and people from different professions.

But as with every moment of revolutionary change, the Internet revolution raises many challenges and challenges for the legal systems around the world. In what way will existing legal structures be revised to encourage effective trade practices while promoting innovation? How are we going to ensure that the law reflects the social principles that outweigh certain interests? What are, in particular, the appropriate roles of both the public and private sectors in resolving these issues? And several legal scholars — including David Post, James Boyle, Lawrence Lessig, and others — have asked in depth about the legal connection to the Internet..

Unit 1: Legal Framework of Cyberspace
Unit 2: Privacy and Censorship
Unit 3: Net Neutrality

Unit 1: Legal Framework of Cyberspace

Contents

1.0 Introduction

Over the past two decades, cyberspace systems have been increasingly focused on a wide spectrum of activities and processes. With this growing societal reliance on cyberspace comes the need to decide how current international legal norms and principles are implemented in cyberspace's boundless and complex world. While academia and government are exploring these issues, there is consensus that international law applies, but the question remains how it applies?

The maturity model addresses international issues in several ways. It was in the 2017 revision of the model that the specific issue of international cooperation in regulatory and legal frameworks became "its own factor" where it had previously been under the factor of the "criminal justice system." Indeed, at the highest level of maturity in this area, "participation in the development of regional or international cybersecurity cooperation agreements and treaties is seen as a priority."

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the advent of the Internet
- describe the nature of the Internet
- discuss Internet Infrastructure.

3.0 Main Content

3.1 Definition of the Advent of the Internet

The 'space race' was seen as a stimulus for personal computer production, with the notion that the US had to reduce the size and weight of on-board computers to offset Soviet rocket power. The relationship between race-to-Internet space is less well-established but can be equally important.

The idea of a decentralized computer network has been discussed in several countries , including the United Kingdom, but a realistic implementation was created in 1964 with the availability of significant funding from ARPA. The theory was that the telephone control centers would be the main targets of attacks, and that conventional telecommunications networks would become unusable.

Message would be sent on its way and transmitted from node to node until they all reached the desired destination, where the message would be reassembled. Although packets are routed in roughly the same direction, the particular route a packet takes depends on the chances and availability of the network. If this affects one portion of the network, the packets will be diverted to other parts.

3.1.1 Nature of the Internet

Where are the Websites? Today's Internet is a technology which millions of surfers use to connect millions of computers around the world. The performance rate for this technology differs from preceding technologies such as telephone, radio, or television quantitatively and qualitatively. The Web is a single network incorporating all information, voice, and visual as digital content. The Internet is called 'push and pull technology' providing a method of contact.

However, the early generation of users of social 'netiquette' actions based on mutual trust and conditioning will also change in the different stages of internet history. The modern ignorance of this 'free public space' is

frequently debated on topics such as cyber-terrorism and cybercrime, rendering the current cyber law jurisprudence and the key 'knowledge access' discussion. '

Except in the endless miles of electronic loops, fibre-optic cables, and silicon chips that make up our computers and networks, cyberspace does not exist physically. Cyberspace, by its very definition, is both anywhere and none. Cyberspace is where we are, whether we are in the center of our minds on the phone with a loved one all over the world. If we watch a movie or wear headphones, then we're in cyberspace.

3.1.2 Internet Infrastructure for Data Transfer

The Internet is the result of the fundamental concept of network engineering with its miracles of connectivity: Keep It Simple.
Any device that is connected to the Internet can do a few, very simple tasks very quickly.. Complex functionality is accomplished by connecting millions of comparatively simple systems together. The Internet is essentially an ingenious messaging network, since it is so easy.

How does Information technology affect the Legal Framework of cyberspace?

3.1.3 Internet and Society

The Internet has revolutionized our way of life, of working and of communication. It has also altered society's way of thinking and behaving. Most of the deviant behavior that may occur in cyberspace isn't special or uncommon for us, but the sense in which this occurs is quite different and needs to be discussed separately.

The Internet is a resource that remains poorly understood due to the change in the speed of our current knowledge climate and the lack of sufficient Internet science studies available.

3.2 Law and Technology

Human history in a sense is a story of technology from flint stones to genetics. The tribulations and triumphs of such a journey that will continue in the future have one thing, constant in its heart - "the laws that govern them." Technology is defined as a 'set of refined processes' resulting in various application of daily use in our lives, in its fundamental construction and description, appears to be a harmless marvel.

Technology became an instrument of progress in society. There was no need for traffic signs and police officers and legislation to control vehicles before the vehicles arrived. In the Late Middle Ages copyright law was created in reaction to the invention.

Technologies are the result of creative creativity by environmental , financial or cultural powers, such as authoritarian regimes, productivity-enhancing economic pressures, or political and military factors such as warfare, or environmental and demographic challenges, placed upon a given society. Technology, law, economic conditions and practices , social interactions, and cultural principles are specific systems or environments in which individuals conduct themselves and with others.

Legal adjustment to the technical choices has been slow. It is agreed that information, incentives, and options are generally positive; there are opportunities for I to prohibit or restrict the use of modern technologies for no good reason, or (ii) to injure people by misuse of technology. Law which made sense in 1850 or even in 1950 could be unsuitable for the challenges and opportunities of today.

In your own words, how would you define cyber law?

3.3 Cyber Law

In frequently spoken conferences, fora and symposia, the word cyber law has gained wide recognition. For academic settings, technology and law centres, Cyber Law and Research & Son, and so on. The key issue is that words like that are used to describe a particular research group. Or simply a common use, without tackling just what the branch of law is. Was this ever changing, or is it common practice to come up with a glamorous prefix or suffix to identical current laws?

Law, in its conventional sense, is only one of those tools, an order backed by a primary behavior-oriented hazard. The general argument is that legislation will affect all other devices that regulate their own actions and can serve as instruments of law. The choice of instruments depends on their effectiveness. However, most importantly, the potential would also raise a query about worth.

 Discussion

Discuss the difference between law and technology and cyber law.

4.0 Self-Assessment Exercise(s)

1. What are the key standardised elements of Internet Protocol IP?

   i) A common method for breaking down any transmission of data into small chunks, called "packets."
   ii) A unified global addressing system.
   iii) A unique identifier assigned to a Network Interface Controller (NIC) to be used in a segment of the Network as a network address.

   a) ii and iii
   b) i and ii
   c) i and iii

2. The Internet is an instrument that remains poorly understood due to the change in pace in our current knowledge environment and the lack of adequate availability of empirical studies on the Internet. True or false?

5.0 Conclusion

1.0 In today's world, cyber systems provide stability with the government's formulated internet policy leading to its illegal use, the internet along with making life easier with economic activities such as purchasing, selling, online transactions, and social networking brings with it many challenges. The Internet has streamlined business processes such as sorting, summarizing, coding, and editing. Cyberspace refers to an ever-evolving global and complex environment defined by the combined use of electronics and electromagnetic spectrum to construct, store, modify, distribute, transfer, remove, use, erase, notify and interact with physical resources.

6.0 Summary

We have defined the legal framework for cyberspace in this unit, as well as the underlying reasons for the Internet legal framework for cyberspace. The emergence of the Internet is debated, and the presence of the internet. Cloud data collection, cloud and network information technologies. Often mentioned is regulation. And Cyber and Engineering regulation. The next unit will reveal the positions of privacy and Internet censorship.

7.0 References/Further Reading

Benkler Y. (2016) Rules of the Road for the Information Superhighway; Electronic Communications and the Law. St. Paul, Minnesota: West Group Publishing Co.

Black S. K. (2012). Telecommunications Law in the Internet Age. London: Morgan Kaufmann Publishers.

Cairncross F. (2017) T*he Death Of Distance: How The Communications Revolution will Change our Lives*. Boston: Harvard Business School Press.

Ibikunle,. F, Eweniyi. O, (2016) "Approach to Nigerian Cyber Security Issues and Solutions." International Journal of Cognitive Research in Science, Technology and Education (IJCRSEE).Vol.4 no 8 pp 7130-7139.

Stinissen, J. (2015). A legal framework for Ukrainian cyber operations Geers, Cyberwar in perspective: Russian aggression against Ukraine Tallinn: NATO CCDCOE Publications, pp123–134

Unit 2: Privacy and Censorship

Contents

1.0 Introduction

Will increased privacy expectations, surveillance concerns and online crime access have an impact on people's level of opposition to dual-use technologies such as the Dark Web? If they do, then how much does the baseline levels of Dark Web hostility actually affect those factors? Do concerns about privacy and censorship get compounded in regimes with extreme restrictions on the Internet? People may use technologies that grant anonymity to protect their privacy from government officials, political rivals, trolls, data-hungry businesses and even Internet service providers. People in highly authoritarian regimes, including the Tor Browser, can also switch to Dark Web technologies that offer anonymity.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the relationship between Privacy and Censorship
- examine the factors affecting internet privacy concerns
- identify the major consequences of internet privacy concerns.

3.0 Main Content

3.1 Definition of Internet Privacy

What is privacy on the Internet? In many jurisdictions privacy is a fundamental right under the law. I see this as a natural right and take the definition of privacy as "the right of individuals to control or influence what information they may collect and store, and by whom and to whom that information may be disclosed. There are many more dimensions to privacy, such as the philosophical or economic privacy perspective.
Internet privacy concern has various contexts in which it can be found. With this context in mind, there are certain aspects of privacy concern that must be taken into account. The biggest of these aspects is that direct marketing is offering the consumer a benefit in exchange for their private information. That is to say, while the consumer is giving up information about himself or herself, in return for that consumer to receive marketing communication, which is personalised towards him or her.

3.1.1 Internet Privacy Concern

What are those elements of Internet Privacy Concerns? As seen earlier, when defining privacy, certain aspects pertained to that of information privacy. What eventual repercussions could be possible if one's privacy were not respected, that is to say, public humiliation and or harm to one's self-identity?

From this, we can gain an understanding that most individuals are afraid of their privacy and any information which can negatively affect them. This is the area of privacy concern: an individual's concern over their privacy and how to protect their best interests. .

3.1.2 Factors affecting Privacy Concern

What factors affect privacy concerns on the internet? The factors affecting a consumer's level of privacy are the most worrying in this respect. Such different factors Castañeda and Montoro grouped into four categories. Intrinsic features of the customer; perceptions, beliefs and attitudes of the customer towards the control mechanism; variables related to the Website; and variables of the situation.
What are those factors affecting internet Privacy Concerns?

3.2 Internet Censorship

There have been attempts to censor media throughout the history of human civilisation. Nearly all media types, from print to digital, are somewhat subject to censorship. Cyberspace isn't exempt from censorship practice. Internet censorship is, in fact, a problem that is widespread worldwide, not just restricted to some countries. Villeneuve claims that – the number of countries censoring and tracking Internet usage by their people has increased.

Why is there Internet Censorship? There are many reasons why the Internet censorship exists. These include social assistance, protection of the culture and dignity of a nation's freedom, economic concern and legal and political reasons.

Firstly, Internet censorship acquires some social legitimacy from the general public's viewpoint. Public opinion polling with Zhao, J. They have repeatedly demonstrated that many accept censorship in specific situations such as pornography, cyberbullying and hate speech as appropriate.

 Discussion

Discuss the difference between internet privacy and censorship.

4.0 Self-Assessment Exercise(s)

1. What are some of the moral reasons for protecting personal data?
   Answer

   i. Informational inequality
   ii. Informational injustice and discrimination

2. _____ is a fundamental right under the law in many jurisdictions.

   Answer: Privacy

5.0 Conclusion

In this unit, internet privacy, elements of Internet privacy concern are covered. The factors affecting internet privacy concerns and why internet censorship exists are also discussed. Also, the major consequences of internet privacy concerns are identified. Finally, the privacy knowledge and factors influencing privacy knowledge, as well as the role of censorship, privacy, and laws on the internet, are covered.

6.0 Summary

In this unit, we have defined the internet privacy, elements of Internet privacy concern. The factors affecting internet privacy concerns and why internet censorship exists are also discussed. Also, the major consequences of internet privacy concerns are identified. The privacy knowledge and factors influencing privacy knowledge, as well as the role of censorship, privacy, and laws on the internet, was also discussed. The next unit is going to expose you to roles played by net neutrality.

7.0 References/Further Reading

Castells, M. (2011) The Internet Galaxy-Reflections on the Internet, USA: Oxford University Press.

Joel, R. (2017). "Using Internet Privacy Technology: Adapting Data Protection Labels and Filters." Lex Electronica, 3(2), pp. 255–265, 2017.

Villeneuve, N. (2007). "Index on Censorship for Resistance Techniques," 36(4), 71–85.

Zhao, J.(2018). "In contemporary China, a snapshot of Internet regulation: censorship, profitability and accountability." China Media Research, 4(3), 37–42

Unit 3: Net Neutrality

Contents

1.0 Introduction

Net Neutrality is the principle that any point on the network can connect to any other point on the network, without any discrimination depending on the origin , destination or data type. The concept is the foundation of success on the Internet. Net neutrality is essential for creativity, competition and the flow of free knowledge. In particular, Net Neutrality allows the Internet to establish new ways of practicing civil law, such as freedom of expression and the right to access and pass on information.

Since the inception of the Internet, its operation has been ensured to have governing principles that provide non-discrimination requirements in all performance dimensions relevant to it. This is similar to what conventional telecommunications services, such as the telephone network, are getting. This is mirrored in figure 1.1.

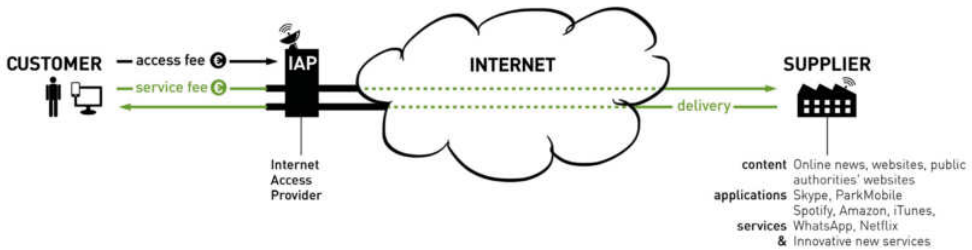


Fig. 1.1: Open Neutral Access Model

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- examine what is meant by Net Neutrality
- explain why neutrality is usually violated
- discuss the policies of ISPs to ensure that all users are treated equally.

3.0 Main Content

3.1 Definition of Freedom of Communication in the Digital Era

The principle of net neutrality that is most widely known is that Internet users can connect to any other point in the network. Users are able to create access and use any content, service or application they choose without being discriminated against, restricted or restricted by those running the infrastructure.

Why are we dealing with internet service providers? Internet access providers help us connect, browse the web or transfer files over the internet, make our websites globally accessible and use services such as email , social media or cell phone. Everyone, of whatever size and style, can participate globally, in whatever capacity, and in all organisations. Everybody can access and offer the services.

Example
Let's say you want to watch a video online: link to the Internet, open your browser, and navigate to your favorite video service. This is possible because your options are not sought by the access provider to limit. Instead, without Net Neutrality, you may find that your link to video service A is being slowed down by your access provider in such a way that you can not view the video. At the same time, you 'd still be able to quickly connect to Video Service B and perhaps view exactly the same content.

How will that do it for your service provider? There are lots of reasons for this. For example, the internet access provider might have a) signed an exclusive agreement with this other video network or b) offered their video services, and thus would like to allow you to use them instead of the service you originally preferred.

3.2 Why is Net Neutrality violated

There are many reasons why we don't respect Net Neutrality. Among those that are most frequent are::

3.2.1 Access Providers Violate Net Neutrality to Optimise Profits

Some Internet service providers are claiming the right to block or delay Internet traffic to their commercial advantage. In addition to controlling Internet connections, Internet access providers are also increasingly starting to provide content, services and applications. They are increasingly searching for the power to become internet "gatekeepers." For example, the Netherlands telecommunications access provider-KPN-tried to get their customers to use KPN's text messaging service instead of web chat services by blocking these free services.

Another notable example of discrimination is the blocking of Internet telephony services by T-Mobile (Voice over IP, or VoIP in short), given by Skype, for example, to give preference to the services offered by their own and their business partners.

3.2.2 Access Providers Violate Net Neutrality for Privatised Censorship

In the UK, blocking measures by access providers have frequently been misused to block unwanted content. For instance, on 4 May 2012, the website of anti-violence advocates "Conciliation Resources" was accidentally blocked by child protection filters on UK mobile networks.

Another example is Virgin Media. The company provides access to the Internet and increasingly uses Deep Packet Inspection Virgin is now using this same privacy-invasive technology to police their network in an attempt to protect its own music business. In all of these cases, private companies police their users' connections to censor what they guess may be unwanted content.

3.2.3 Access Providers Violate Net Neutrality to Comply with the Law

Governments are increasingly demanding access and service providers to restrict certain types of traffic, filter the Internet and monitor it to enforce the law. A decade ago, the Internet was filtered and censored worldwide only by four countries. Today, they are in over forty. Web blocking has been implemented in Belgium, Franc, Italy, the UK and Ireland for example in Europe. This is done for reasons as varied as the defence of national gaming monopolies and proven futile attempts to preserve copyrights.

Some lawmakers lobby for net neutrality, others seeking filtering or blocking for law enforcement purposes. However, it is paradoxical to

establish legal incentives for operators to invest in monitoring and filtering or blocking technology, while at the same time insisting that they do not use this technology for their own business.

3.3 Net Neutrality Flaws

Net neutrality rules make Internet networks illegal to sell "fast lanes" to anybody who wants to pay extra. That means everyone is getting an equal share of the bandwidth, but it overlooks situations where "fast lanes" can help save lives. An example of this is telemedicine, which is not yet practiced because no one wishes to risk remote surgery when other streams of online video can congested.

A Japanese study shows that remote surgical collaboration with a dedicated internet link is feasible in real time; however, such collaboration is futile with the net neutrality legislation at stake. Another emerging net neutrality debate is how to limit the quality of the services. Standardizing the price of broadband services sounds fair but the issue is that they can become extremely complex.

Hahn and Wallsten have used for example the regulation of natural gas. The gas prices were initially divided into five thirds. Each had a regulated price, depending on when the gas was being sold and where. But by the time the 1978 Natural Gas Policy Act was passed there were 28 different gas pricing categories. Finally, they concluded that it is difficult to develop a flexible pricing system and that these regulations could have a major impact on the economy's welfare.

Assignment 1

Identify and address the freedom of expression protected by this unit in the digital age.

4.0 Self-Assessment Exercise(s)

1. List and explain a few points to safeguard net neutrality.

   Answer
   i. The Internet must be kept neutral and open.
   ii. Accessibility between all internet-connected endpoints must continue without any restriction.

2. _____ is defined as the principle that Internet users can connect to any other point in the network?

   Answer: Net Neutrality

5.0 Conclusion

With reasons in this segment, we addressed the net neutrality that in the digital age demands freedom of communication, and why net neutrality was violated. Such factors include providers of access breaching Net Neutrality for benefit optimization; providers of access breach net neutrality for privatized censorship; and providers of access breach net neutrality for law enforcement. Finally, there has been talk about vulnerabilities in net neutrality.

6.0 Summary

In this unit, we defined the digital-era net neutrality that includes freedom of communication. We have discussed why breaches of Net Neutrality occur. The reasons are access providers breach net neutrality for profit optimization; access providers breach Net Neutrality for privatized censorship and access providers breach net neutrality for law enforcement. Lastly, it tackles flaws in net neutrality. The next unit will expose you to the Advance Fee Rule on Fraud and Other Fraud Related Offenses (Amendment).

References/Further Reading

Eijk, N. Van, (2011). "About 1.0, 2.0, 3.0 and 4.0 Network Neutrality." Computers and Law Magazine, 21(6), pp.1-4.

Robert W. Hahn. and Wallsten, Scott (2011).The Net Neutrality Economics. "The Voice of Economists: Vol. 3: Iss. 6. Article 8. The Berkeley Electronic Press Nov. 2011.

Wu, T. Wu. (2013). "Network neutrality, broadband discrimination" Journal of Telecommunications and High Technology Law, 2, 141.

Module 2: Cyber Law in Nigeria

Module Introduction

Welcome to Nigerian cyber-law. This module will be completed within 10 hours; it will be supported with videos and exercises which will allow you to learn Nigeria's most important cyber law concepts. The module is the second in the course which aims to present Nigeria's cyber law. You'll also learn about the Advance Fee Fraud and other fraud related offences (amendment) act in a simple way. The Cybercrime Act and the Evidence Act will be discussed in greater detail. Finally, you'll also learn about the Nigeria Data Protection Regulation, the cybercrime agenda and strategy.

Unit 1: Advance Fee Fraud and other offences related to fraud (amendment) Act
Unit 2: Cybercrime Act
Unit 3: Evidence Act
Unit 4: Nigeria Data Protection Regulation, cybercrime policy and strategy

Unit 1: Advance Fee Fraud and other offences related to fraud (amendment) Act

Contents

1.0 Introduction

Fraud is a form of delusion that involves the theft of money using criminal deception, misrepresentation, dishonest artifice or theft trick to the advantage. It involves taking other people's money, without their knowledge. Elaborate fraud is merely artful, and it is difficult to trace this form of activity. It usually involves several companies, business directors' activities, large amounts of money or assets being transferred – sometimes offshore – to other corporate entities, or luxury cars or homes, antiques, yachts, etc.

In this regard, funds are taken out of the company or government structures where they ought to be and put into someone's pocket or corporate structure or trust or Swiss Bank account, where they ought not to be. It may also involve transfers of funds from investors' accounts to the account of the perpetrator. Often the money chain is difficult to trace, as it moves around the world.

This type of fraudulent activity occurs very often, far more than the common fraud perpetrated against companies and governments. In recent times, one particular kind of fraud has surfaced internationally; Advance Fee Fraud (AFF) that is also known as the 419 scams.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- define the concept of crime
- Describe the Advance Fee and other fraud-related offences (amendment) Act
- explain the evolution of Advance Fee Fraud.

3.0 Main Content

3.1 Definition of Crime

Schmalleger defines crime as behavior that violates a state, federal government, or local jurisdiction's criminal laws that have the power to formulate such laws. Tappen describes crime as an deliberate act in violation of criminal law committed without protection or justification and prosecuted as a felony or misdemeanor by the state.

Sutherland said it is essential characteristic of crime that the state bans behavior as an injury to the state and against the state for which the state can react through punishment. Reid defines crime in the same vein as an international act or omission that violates the statutory criminal or case law and is punished by the state for it.

3.2 Fraud

Jones describes fraud as "... an illegal and intentional misrepresentation that causes actual or possible harm to someone else." This definition allows for the distinction of four elements of fraud: unlawfulness, motive, misrepresentation and harm.

1. A misrepresentation happens when one party makes a representation to another that there is a fact or set of facts that are in fact fictitious.
2. Intention applies to practice, in compliance with South African law. It must be proved that the action contravened statutory prescription and at the time the perpetrator was aware of the fact. And
3. The law imposes two intentional requirements, namely intention to mislead and intention to defraud.
4. The law demands that the misrepresentation result in harm.

What is the difference between these four elements of fraud?

Differences between the four elements of fraud
Unlawful activity in relation to an individual or association shall mean any action taken by that individual or association, whether by committing an act or words, spoken or written, or by signs, or by visible representation or otherwise.

However, misrepresentation liability may be predicated on misrepresentation which is more than deliberate deception. Furthermore, misrepresentation can be divided into negligent misrepresentation, based on careless misrepresentation, and innocent misrepresentation, backed by strict liability and express warranty justification. Therefore the rule of misrepresentation is far broader than the cause of fraud.

What distinguishes a criminal misrepresentation from a civil misrepresentation is a Community condemnation judgment that accompanies and justifies the imposition of a criminal sanction. In other words, a criminal misrepresentation "is conduct which, if duly proven to have occurred, will incur a formal and solemn pronouncement of moral condemnation of the community.

In such harms caused by the negligent act in fact and in the immediate vicinity, where the negligent misrepresentation of the defendant, however, causes only the pecuniary damage of the plaintiff, as is usually the case in

the sense of employment, the claim of negligence may still be held, but the scope of the defendant's liability may be narrower than in the proximate cause of the conventional. In particular, the defendant's responsibility will be limited to those persons for which the defendant intended to provide the information for benefit or guidance, as well as those persons on which the defendant intended to rely.

3.3. Advance Fee Fraud

On 1 April 1995 in Nigeria new legislation came into force: the Advance Fee Fraud and Other Related Offenses Decree (No. 13 of 1995). This legislation prescribes three forms of behaviour: buying property under false pretences, doubling, washing and minting money.

Advance Fee Fraud is therefore defined as an advance payment to a fraudster by a victim to allow him to participate in a much larger financial transaction, which he assumes will either bring him income or lead to credit extending to him. In this case, the victim is asked to pay some type of advance fee such as "transfer tax," "performance bond" or "chemicals buy money." If the victim pays the advance fee, there are often other "complications" that involve many more advance payments before the victim fails or runs out of funds.
Advance Fee Fraud is a crime involving, at some stage (as described above), misrepresentation, corruption and bribery, forgery and money laundering, extortion , kidnapping and even murder of victims.

3.3.1 Corruption and Bribery

Corruption consists of awarding or offering a benefit of some nature, unlawfully and intentionally, which is not legitimately due to anyone to whom any power has been given or who has been charged with any duty, in order to induce the latter to carry out or withhold some act involving such power in the future or to compensate the latter for some act or omission in the past in relation to such power.

The World Bank and Transparency International call corruption "... the abuse of public office for private benefit." As such, it involves the unethical and illegal actions of public service officials, both politicians and civil servants, whose positions generate government incentives for them and their accomplices to diversion money and property. Corruption distorts resource allocation, and policy efficiency.
The evolution of corruption has many reasons, and they differ from country to country. Poorly designed and implemented policies, services and initiatives, poverty, income inequality, insufficient remuneration for civil servants and a lack of accountability and transparency (Sherman and Kelly) are among the contributing factors.

3.3.2 Forgery

Forgery is committed when a false document is made with the intention of defrauding another's actual or possible bias, of course unlawfully. For example, the fake document is intended to imitate another document or create the illusion that it was written by someone other than the actual writer (e.g. ID documents, official letterheads, company and government seals, signatures, passports, etc.).

The suspects in the AFF case use skilled forgers to rob signatures from actual business owners and government officials. Corporate and government letterheads and fake companies are created to provide the banks with false information to open accounts where illegal funds can be transferred or deposited into them.

3.3.2.1 Money Laundering

Most of the money earned by organized crime comes from illegal sources, and criminals are unable to reveal their income or sources. Before spending or utilizing those funds they must give the money an aura of legality. Money laundering is called conversion.

3.3.2.2 Extortion

Extortion is characterized as money / property obtained from another person through abuse, through means of their office, by real or threatened coercion, fear or violence, or by the acceptance of a fee by corrupt public officials when they are not entitled to that fee.

3.4. Nature and Forms of Advance Fee Fraud

Advance Fee Fraud is an organised crime that is complex, and it is a relatively new universal threat. Yet, it has still not been debated or properly understood by those outside state organisations, such as academics, analysts and the public. Those inside the state also had to come to terms with a new threat, in a short period of time, their understanding of this type of organised crime is thus limited.

It is precisely due to the covert activities of organised crime syndicates that the public, in particular, is not aware of the destructive and corroding impact that it has on society. Not only does it contribute to the high crime rate, but also corrupts law enforcement officials and threatens the very legitimacy of the state and its efforts to defeat such organised criminal activities.

In this situation, the victim would quite rightly be apprehensive that he/she had aided and abetted some criminal activity and would also be reluctant to make the fact of his/her gullibility public. Thus the perpetrator can carry out the scam repeatedly, sometimes involving the same victims, while the police find it difficult to locate witnesses and secure evidence.

3.4.1 Nature of Advance Fee Fraud

This fraud mainly involves the payment of advance fees in the form of tax, brokerage, and bribes and so on, under the pretence that such payment is needed to consummate a business deal, which the perpetrator knows will never materialize, as the objective is to defraud the other party.

Advance fee frauds cases that have been discovered to date have taken a variety of forms. All entailed that victims were approached by letter or, recently, by electronic mail, without any prior contact.

Victims' addresses are obtained from telephone and email directories, business journals, magazines or newspapers. The perpetrators generally describe the need to move funds out of Nigeria and seek the assistance of the victim to provide bank account details of an account in an overseas country as well as so-called administration fees to facilitate the transactions. The victim is offered a commission, which could be up to 40 per cent of the capital involved.

3.4.2 Forms of Advance Fee Fraud

It should be remembered that the attacker's creativity limits confidence scams on AFF. Nevertheless the ideas share a common thread. Sometimes the offers are unsolicited, emphasizing the urgency and anonymity of the contract, and allowing the individual to pay the different government and legal fees and taxes before getting what turns out to be non-existent funds.

New variations of these scams are constantly being developed, but among those main categories are the most common types of these fraudulent business propositions:

1. Transfer of funds from over-invoiced contracts
2. Contract fraud (C.O.D of goods and services)
3. Conversion of hard currency (black-money, money cleaning or "wash wash")
4. Sale of crude oil at below-market prices
5. Purchase of real estate
6. Disbursement of money from wills (benefactor of a will)
7. Held for ransom / Kidnappings and murder

 Discussion

Do a descriptive analysis of the phenomenon of Advance Fee fraud, and then explain the crime.

4.0 Self-Assessment Exercise(s)

1. one of the characteristics of Advance Fee Fraud is:
   Answer
   Corruption and bribery
2. Advance Fee Fraud is a crime involving only corruption, bribery, forgery, money laundering, and extortion.. Yes or No?
   Answer
   No

5.0 Conclusion

Crime and fraud were identified in this unit; the basis for corruption and bribery was clarified in the Advance Fee Fraud. Finally, forgery has also been described to help you fully understand the nature and forms of Advance Fee Fraud.

6.0 Summary

In this section, you learned more about crime and fraud; in addition to the unique relationship between corruption and bribery, Advance Fee Fraud was thoroughly clarified. Finally, in order to fully understand the nature and forms of Advance Fee Fraud and Other Fraud-related Offenses (Amendment) Act, forgery was also described.

7.0 References/ Further Reading

LAMP, A. (2012), "Official reporting of complex commercial fraud." Conference proceedings No 10 The Australian Center for Complex Criminology Commercial Fraud pp. 68-74

Jones, M. (2013). "Nigerian Crime Network in the United States" *International journal of offender therapy and comparative criminology* vol. 37 no.1. Spring, NY: Guilford Press

Irish, J. & Ohobosheeane (2013). *Penetrating State and Business Organised Crime in Southern Africa.* Vol. 2 ISS Monograph no. 89 November 2013

Sherman, W. L. Mitlon, H. C. And Kelly T. (2013). The Police Team: Seven case studies. Washington, DC: The Alliance for Police

Unit 2: Cybercrime Act

Contents

1.0 Introduction

Attacks against the information infrastructure and the Internet services have already been carried out. Online fraud and hacking attacks are just a few examples of computer-related crimes per day on a large scale. The financial damage caused by the cybercrime is estimated to be huge. In 2007, by some figures, the profit from cybercrime reached USD 100 billion, outstripping the illicit drug trade for the first time.

Deterring cybercrime is an important component of the national safety and essential information infrastructure strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes, and activities aimed at affecting the integrity of critical national infrastructures. This is a shared responsibility at national level that requires coordinated action on incident prevention, preparation, response and recovery by government authorities, the private sector and citizens..

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- define cybercrime
- explain the cybercrime act
- identify the circumstances in which the cybercrime act can be evaluated for adequate deployment and protection.

3.0 Main Content

3.1 Definition of Cybercrime

Cybercrime in a limited sense (Computer crime) includes any unlawful activity driven by electronic operations which threatens the protection of the computer system and the data it generates. Cybercrime in a broader context (internet-related crime) includes any criminal activity committed through the use or intervention of a computer system or network, including crimes such as unlawful possession and the provision or dissemination of information via a computer system or a network..

One standard concept defines cybercrime as any operation where computers or networks are a device, goal, or location for criminal activity. For instance, if the perpetrator used a keyboard to hit and kill the victim, it would cover common crimes like murder.

Another broader definition is provided in Article 1.1 of the Stanford Draft International Convention for the Enhancement of Cyber Crime and Terrorism Protection (the "Stanford Draft"), which states that cybercrime refers to cyber-system acts. Cybercrime may also be defined as computer-mediated activities that may be performed through global electronic networks, either illegal or deemed illicit by some parties.

3.2 Offense against the dignity, honesty and accessibility of computer data and systems

All breaches in this category are directed against (at least) one of the three legal principles of confidentiality, integrity , and availability. Computerization of offenses is relatively new, as opposed to crimes that have been protected for decades under criminal law (such as robbery or murder). Effective prosecution of such crimes includes current criminal legislation not only to protect objects and physical evidence related to abuse but also to expand new legal requirements to cover them.

3.2.1 Illegal Access (Hacking, Cracking)

The offense identified as "hacking" refers to unauthorized access to a computer device, one of the oldest offenses pertaining to computers. Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. That comprise the United States. National Aeronautics Administration and Space Administration (NASA), USA The Pentagon, the Air Force, Facebook, Google, eBay and the German government. Examples of hacking crimes include cracking

passwords for password-protected websites, and circumventing security protection for mobile devices.

But activities related to the term "hacking" may involve preparatory activities such as using outdated equipment or installing software to acquire a password to unlawfully access a computer network. This is in addition to setting up "spoofing" websites that allow users that reveal their passwords and to install keylogging methods based on hardware and software (e.g. "key loggers") that record every keystroke – and thus any passwords used on the computer and system.

This access is used by offenders to commit additional crimes, such as data spying, data manipulation or service denial (DoS) attacks. In most cases unauthorized access to the computer system is just a vital first step.

3.3 Computer-related offences

That category includes certain crimes including the use of a computer program. Such specific offences in the enforcement of moral standards are often not as rigid as in previous categories. The category includes malware, forgery, phishing , identity theft and abuse of the network related to computers.

4.0 Self-Assessment Exercise(s)

1. One of the following is not a motivation of offenders
   a) Interested in circumventing security measures only to prove their abilities.
   b) Hacktivism
   c) Money
   d) Testing penetration

   Answer: d

2._____ refers to unlawful access to a computer system, one of oldest computer-related crimes.
a) Hacktivism
b) Denial of Service
c) Cracking
d) Identity theft

Answer: c

Assignment:
Write a short note on the following Computer-related offences, and submit to your tutor.

1. Computer-related fraud
2. Computer-related forgery
3. Phishing
4. Identity theft
5. Misuse of devices

5.0 Conclusion

Cybercrime and offenses were protected in this unit from confidentiality, honesty, and computer data and systems being available. It was also explained the Illegal access which includes hacking and cracking. Finally, the computer-related offenses and factors that cause the offenses were addressed, as were the ways of overcoming the problems.

6.0 Summary

In this class, you learned about cybercrime and crimes against computer data and information security, honesty and availability. It was also clarified the Illegal access which includes hacking and cracking. Finally, there was a clear discussion of computer-related offences and factors affecting the offenses as well as the way to solve the problems. The Proof Act will be dealt with at the next level.

7.0 References/Further Reading

Benkler Y. (2016) Digital Superhighway Road Rules The Law and Electronic Communications. St. Paul, Minnesota: Groupe West Publishing Inc.

Brown, C. V., Martin E. W., DeHayes, D. W., Hoffer, J. A. (2012) Policy relating to information technology. New Jessy: Lounge with the Prentice

Chisum, D. S. Schwartz, H. F. & Newman P. N. C. A. (2018). *Principles of Patent Law: Cases and Materials*. New York: Foundation Press.

Cornish, R.W. Llewelyn, D (2003), Intellectual Property: Patents, Trademarks of Copyright and Related Rights; London: Maxwell & sweet.

Unit 3: Evidence Act

Contents

1.0 Introduction

The term evidence may refer to a statement of truth, which is established by proof in the first sense. This is often called an "evidential fact." It is evidence in the second context of his possible participation in the crime that the accused was at the time in question at or near the crime scene. Yet, by presenting evidence, the existence of the accused has to be proved in the first sense. The prosecution may, for example, call a witness to appear before the court and make him testify that he saw the accused at the right time in the vicinity of the crime.

Seeking evidence is a jury job. Though the judge is named for some types of cases and in countries without a jury system. The evidence for the fact-finder is not immediately available. When the alleged knife used to commit the crime in question (a type of "true evidence") is presented in court, the fact-finder will see for himself the shape of the knife; he doesn't need to know about it through a testimony from an intermediary.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe opinion evidence
- explain the term "Evidence Act."
- identify the best way to manage the admissibility of electronic evidence in investigations.

3.0 Main Content

3.1 Definition of Opinion Evidence

Evidence of guilt, or proof, as the Black Law Dictionary put it, means confirmation of what the defendant feels, believes, or assumes of the facts at issue, as distinct from his own understanding of the facts themselves.

It has been argued that normally, proof rules do not require a witness to testify as to opinions or hypotheses except in such cases, and these are exceptions to the general rule. One such situation is the calling of a "Expert Witness." Expert witnesses are those who have become [experts] and authority in their field of study, calling or vocation, whether in the field of art, humanities or science, by virtue of their education.

3.2 Fundamental Principle of Witness Evidence

The purpose of calling a witness is to obtain from him or her evidence of facts perceived through its senses. That is, what he saw with his eyes; what language did he or she taste of? How it felt; what it saw with its ears, and how it smelled its nose.

There are, however, cases in which the judge lacks the expertise necessary to draw knowledgeable, reasonable inferences from the evidence arising from the case. The court then makes somebody with the skills needed to do so. The aim is to use the opinion of an expert on the court's evidence to help it pass a proper verdict.

3.3.1 The Expert Evidence Test for Admissibility

The admissibility of an expert opinion depends on:

a. The court's ability to decide the matter without aid.
b. The credential of the expert-whether he or she is a member of a profession; doctor, engineer, pathologist, chemist, etc., his / her professional qualifications.

Formal qualification is necessary but is not a precedent requirement. For example, if learning handwriting has been his hobby, a solicitor may qualify as a handwriting expert. At times, non-expert opinions are acknowledged, for example in areas of recognition or interest. The accused has been charged in R.V. Davies (1967) was disqualified for driving a motor vehicle while drunk;.

A non-expert witness was summoned to provide evidence of his or her intoxicated state or condition, and he spoke of the view he had on the condition of the accused. On the non-expert witness the court expressed the following view:

(i) That the non-expert witness, whether or not the accused took liquor, may state his opinion, but must state the facts on which he relied in forming his opinion;

(ii) He was not an expert, and was unable to say whether or not the accused was fit to drive a vehicle. That was a matter for the trial court to decide, not on the opinion of non-experts or ordinary witnesses.

(iii) A person other than an expert's opinion may be admissible regarding the state or condition of a person, rather than his / her mental health.

3.3.2 Competency of an Expert or Specialist

The Proof Act does not provide us with guidance about how to rate an expert with any degree of certainty. An expert is a person specially qualified in the fields of foreign law, native law and custom, science or art, handwriting and fingerprint analysis. His or her authority shall be determined by the judge. Whether or not he or she has acquired professional knowledge goes to weight, not admissibility. The test of an expert 's relevance is whether he's especially skilled in the given field.

You must first state your qualification, experience , training, nature and duty in relation to your field or office when you are called as an expert witness. These are to persuade the court that you are an expert on the subject that you are about to bear witness to. And also to explain getting the evidence obtained as valid proof.

However, it should be noted that, in deciding whether a person's qualifications require him to be considered a qualified expert, not only the

general character but also the particular nature of the issue on which the expert evidence is required must be taken into account (Ajani v the Customs Controller, 1954).

3.4 Evidence Act of 2011

Section 68
(1) Where a court is required to give an opinion on matters relating to foreign law, native law or tradition or science or art or the identity of the handwriting or fingerprint, it is admissible to give an opinion on that point to persons who are especially qualified under such foreign law, customary law or practice or to science or art or to questions relating to the identity of handwriting or fingerprints.
(2) Experts shall be named individuals with that particular skill as referred to in subparagraph (1) of this section.

Section 67
The fact that any person is of the opinion that a fact in question or relevant to the matter exists or does not exist is irrelevant to the nature of such a fact, except as provided for in section 68 to 76 of the Act.

3.5 Other Instances of Opinion Evidence

There have been other specific subjects of expert evidence, namely:
i) Evidence as to the identity
ii) Handwriting
iii) Other cases

3.5.1 Evidence as to the identity

Evidence as to the identification of a person or a thing is an expression of opinion. Examples are evidence of:

I. A person's general resemblance to a photograph or a member of and identification parade.

II. The memory of goods stolen in comparison with actual goods recovered.

III. The age of a person.

IV. Condition of a person or thing

You can give evidence as to the identification in appropriate cases as an expert or non- expert.

3.5.3 Handwriting

Typewriting is for handwriting. A handwriting expert may compare a document that has been confirmed to have been written by the individual whose handwriting is sought with the document at issue when handwriting or type-writing is in dispute. After conducting such a comparison, the handwriting expert may be called upon to express his or her opinion.

The court will often ask the person whose handwriting is being challenged to write, in the presence of the court, and the court will shape its opinion with or without expert guidance. Sometimes, the witness doesn't need to be a specialist or expert in handwriting analysis.

Suffice it to say that he or she is one:

i. Forms an opinion based on comparison of mind,
ii. Sees or has seen the person (whose handwriting should be compared with) write on specific occasions or and
iii. Is familiar with his writing having seen letters which are supposed to be in his writing or
iv. Having read a document which was supposedly written by the person whose handwriting is in dispute.
v. Is proficient or has given the subject considerable attention and study. The courts received opinions

or expert handwriting proof from :

- Police agent R.V. 12 WACA 58, ONITIRI (1946).
- A solicitor who has been studying fingerprint 10 years R. (1894) V. Silverlock 2 QB 766.
- Handwriting analysts who are specialist trained in the field.
- Someone experienced in analyzing fingerprint impression.

 Discussion

What is the fundamental principle of witness evidence and how has the hearsay rule been relaxed for expert witness?

4.0 Self-Assessment Exercise(s)

1. Expert witnesses are
   Answer:
   Those who, by virtue of their education and experience, have become knowledgeable and authority in their area of the profession, calling, or vocation.

2. The admissibility of expert opinion depends on the following:
   Answer
   i. The court's competence to determine the matter without assistance
   ii. The qualification of the expert.

5.0 Conclusion

It is a basic concept of witness proof that a witness should bear testimony to the truth and not to the reality of his opinions. Opinions may come from the findings of secondary evidence-hearsay. Evidence of opinion, in general, is removed from the proof. But when anything has occurred which is beyond the court's knowledge, proof of opinion is important and admissible. Expert opinion is thus admissible for proving foreign law and customary law.

6.0 Summary

You have learned in this unit what evidence of opinion is and the reasons for its exclusion from facts. The evidence allows for some exceptions to the rule that you must keep to your heart. You learned who could give an expert opinion, too. Any person subject to satisfying certain preconditions may give an opinion on foreign law, native law and custom, handwriting (including typewriting), and impression of fingerprints. You may see instances where scientific and technological progress has extended the spectrum of expert opinion into psychiatrist and psychologist opinion areas.

7.0 References/Further Reading

Afe, B. (2001 *Law and Practice of Evidence in Nigeria.*

Allen & Gush (2004). Evidence U.K.: University of London Press.

Evidence Act of 2011.

Nwandialo, F. (1999). (2nd ed.). *Modern Nigerian Law of Evidence*. Lagos: Lagos University Press.

Unit 4: Nigeria Data Protection Regulation, Cybercrime Policy and Strategy

Contents

1.0 Introduction

Technological advances have led to the achievement of a number of notable milestones. Many of these are in the field of communication and information technology. Over the last few decades, further research and development has culminated in the discovery of revolutionary computer technology enjoying widespread acceptance across the world. The overwhelming penetration of modern computing has left the world ever more dependent on digital technology and networks.

This can be seen in different facets of human civilization including, but not limited to, banking, education, commerce, business, healthcare, socialization and communication. Information about a person's data can only be collected and/or processed with the specific, legitimate and legal consent of a user or subject. Such consent shall not be obtained by deceit, coercion, misrepresentation or unwarranted power.

No permission shall be obtained, granted or accepted under any circumstances which, directly or indirectly, can contribute to the spread of the violation of any child's rights, hate or other anti-social norms.
Any consent given by the data user or subject must also be freely and easily withdrawn at any time, without any explanation for the withdrawal offered. Similarly, where such portability is technically feasible, the data user has the right to the portability of his data.

The collection and use of personal data for science, historical, public interest studies, or other statistical purposes is a recognized essential exception to the above consent law. Where such data are to be transferred to a third

party, however, prior consent must be obtained from the user or subject of the data.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- Explain Regulation on data protection
- Identify policy alternatives for the creation and implementation of national legislation;
- To explain data security and privacy in Nigeria.

3.0 Main Content

3.1 Definition of Data Protection Regulation

In the digital world , data security relates directly to trade in goods and services. By reducing consumer confidence, inadequate protection can cause adverse market effects, and excessively stringent protection can result in companies being unduly restrictive, with adverse economic consequences. Ensuring laws understand the global complexity and reach of their operation, and fostering alignment with other systems, is vital to increasingly Internet-based global trade flows.

The information economy is becoming more popular and promises to give many opportunities, but there may also be some possible drawbacks. Internationally compliant data protection laws are ideal as a way of creating a more stable atmosphere for all parties involved in the digital economy and building trust online.

To promote potential benefits, the data protection regulations need to carefully balance the changing requirements and possibilities associated with those changes. Drafting and enforcing data protection laws are confronted with many challenges. This study focuses on seven areas where action is needed in particular.

1. Fixing coverage gaps
2. Addressing Modern Software
3. Managing transnational data transfers
4. Balancing data security and surveillance
5. Enforcement strengthened
6. Determining competences

7. Managing the load on enforcement

In-Text Question(s)

1. Explain the growing importance of data protection.

Legislation on data protection dates back to the 1970s, reflecting concerns about the emergence of computer and communication technologies, with their ability to process large volumes of data remotely. Although different national , regional and international initiatives have adopted radically different regulatory strategies, there is a remarkable degree of harmonization and coherence around the core principles that underpin them, as mentioned below.

Common requirements include the need to provide every processing operation with a legitimate objective, achieved either by agreement or any other justification designed to take private and public interests as opposed to it. Another core principle is the obligations regarding the quality of the processed personal data , which requires accurate , complete and up-to - date data. Compliance with this maxim should be mutually beneficial for both the treatment of subjects and processors.

Data security is of crucial importance to the position. Security measures should protect against accidental loss or destruction of data, whether physical, logical or organizational, from deliberate misuse. Similar to data quality problems, effective data protection implementation will balance the needs of individual data subjects, the personal data processing agency and indeed society as a whole.

2. What are the trade implications of data protection?
   Divergent regulatory approaches lead to disparate levels of jurisdictional protection. This, in turn , leads to the need for legal controls on cross-border flows of personal data between jurisdictions, to avoid circumventing the laws of the more protective regime and to eroding the privacy rights of individuals.

   Although the possible need for regulation of cross-border data flows for privacy purposes is obvious, the implementation of these controls in an increasingly interconnected world is extremely challenging. ICT technologies, such as cloud computing, make it much more complex, with processing agencies not actually understanding where the data is stored. Although the answer may ultimately be a technological one, increased harmonization of law and regime would significantly reduce the chances of friction over cross-border data flows.

   Data security is a growing sector, particularly as the digital / knowledge economy expands. As more business models and

practices move into the digital platform and data are increasingly shared and exchanged on an international scale, they are intensifying their relationship with international trade. Since data is collected, digitized, processed and transmitted on a truly global basis by a multitude of parties, restrictions and data-related regulations that directly impact global commerce.

3.2 Policy Options for Developing and Implementing National Laws

There has been an increase in the number of national data security legislation but there are still major gaps. Some countries in this region have no laws, some have partial laws and some have obsolete legislation that needs modifications. The study proposes key policy choices for developed countries, updating or amending their data security regulations. Governments should lay down regulations for those countries that do not yet have specific legislation in place that would cover data collected by the government and private sector and eliminate exemptions to achieve broader coverage.

There is strong support for the establishment, where possible, of a single central regulator with a combination of supervisory and complaint management functions and powers. Furthermore, the trend is to extend enforcement powers and increase the size and scope of fines and data protection penalties.

3.3 Data Privacy and Protection in Nigeria

Data has become increasingly relevant in this modern digital age, with data being called the "latest oil," and data privacy and protection have taken center stage. At present, a number of countries are taking steps to ensure proper protection of their citizens' data and privacy. The European Union released a General Data Protection Regulation (GDPR) in May 2018 to address data security and its associated abuses.

Ideally the law will foster increased foreign investment and Nigerian jobs. Despite Nigeria's rapid growth in technology and digitisation, no substantive legislation has been introduced to protect Nigerian people's data.

Article 37 of the Constitution establishes the '... This safeguards and preserves the privacy of people, their residences, emails, telephone calls and telegraphic communications ...' and other sector-specific data protection regulations, such as the NCC5 Regulations on the Consumer Code of Practice and the CBN6 System for Consumer Security, seek to secure data handling and transmission.

The National Development Agency for Information Technology ('the Agency') is the principal regulator responsible for monitoring electronic governance and controlling the use of electronic data and other forms of electronic communications transactions in Nigeria.

3.4 Cyber Security Policy and Strategies

In modern times, companies, governments, programs, associations or countries, as the case may be, are prevalent in developing and regulating policies and strategies that are relevant to all aspects of their activities and prolong their life expectancy.

Effectiveness of any organizational effort depends on the immediate goals set to achieve it, as well as the strategies prescribed and implemented to attain those goals. Both documents are most often intertwined with the objectives they are aiming to achieve, and are therefore often considered the same.

"National Cyber Security Strategy (NCSS) is the nation's readiness strategy to deliver cohesive measures and strategic actions to ensure the country's presence in cyberspace, safeguard critical information infrastructure, build and nurture trusted cyber communities," according to the Nigerian National Security Adviser 's Office (2014).

 Discussion

The effectiveness of any organizational effort depends on the immediate objectives set for achieving it, as well as the strategies prescribed and implemented for achieving those goals. Discuss.

4.0 Self-Assessment Exercise(s)

1. What is data protection?

   Answer
   It directly related to trading in goods and services in the digital economy

2. Big data analytics is _____
   Answer

it is a methodology for analysing large data sets to reveal patterns, trends, and associations.

5.0 Conclusion

Data protection regulation has been explained in this unit as a basis for policy options for the development and implementation of national legislation. In Nigeria, data privacy and protection were defined for organizational initiative success. Finally, it also explained cybersecurity policy and strategies..

6.0 Summary

In this class, you learned about the regulation of data security and the opinion on policy options for creating and enforcing national legislation. In Nigeria the use of data privacy and security was implemented for the organizational initiative's success. Finally, it also addressed cybersecurity policies and techniques.

7.0 References/Further Reading

World Economic Forum. (2013, February). 'Unlocking the Value of Personal Data: From Collection to Usage'. Retrieved from http://www3.weforum.org/docs/WEF_IT_ UnlockingValuePersonalData_CollectionUsage_

Hertzel, D. A.(2018). 'Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online'. Federal Communications Law Journal, Vol. 52,(2018), pp. 429 – 451.

Kathryn C. M. (2018). Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet. MIT Press, p. 89.

Birenz, J. S. (1998). 'Caching World Wide Web Sites', Practicing Law Institute, p. 475.

Campbell, A. J.(2017). Should Government Regulate Advertising to Children on the World Wide Web?'. Gonzaga Law Review, Vol. 33, No. 331, pp. 320.

Module 3: Cyberlaw: International Perspective

Module Introduction

Crime involving the use of standalone or interconnected computers has taken so many dimensions. These dimensions tend to differ a bit from one country to the other but generally are the same in most cases. Computer crime, e-crime, electronic crime and even cyber crime are nomenclature for the defilement of criminal law with the use of computer technology. The laws that relate to the internet or internet-related technologies are called Cyberlaw. Cybercrime committed by an attacker in one country might have its target in another, and that called for the need to have an international law governing the crime.

Since most computer-related offences have an internal dimension, 26 member countries in 2001 convened in Budapest. They signed the Council of Europe Convention on Cybercrime which creates criminal policy that is common to them which is aimed at protecting their society against cybercrime. The policy, inter alia, will adopt ten required legislation and foster international cooperation. This legislation covers treaty and investigation as it relates to cross-border crime.

Unit 1: United Nations and International Telecommunication Union (ITU) Initiative
Unit 2: Council of Europe-Budapest Convention on Cybercrime

Unit 1: United Nations and International Telecommunication Union (ITU) Initiative

Contents

4.0 Self-Assessment Exercise(S)
5.0 Conclusion
7.0 Summary
7.0 References/Further Reading

1.0 Introduction

In this unit, the common type of computer crime according to the United Nation (UN), the taxonomy of the offences and threats is outlined. The ways of combating this crime will be discussed in detail.

International Telecommunication Union (ITU) is the UN specialised agency for information and communication technologies covering three main areas of activities: radiocommunications, standardisation and development. Before cybercrimes can be reduced or eliminated, all forms of threats need to be known to ease the way to go about it. The use of the computer to perpetrate cybercrime lends its target to the categories of crime it is used for.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe the types of cybercrime
- classify cyber offences and threats
- utilise different initiatives to combat cybercrime.

3.0 Main Content

3.1 Cybercrime Types According to the United Nations

Cybercrimes are categorised generally into five (5) forms. They are:

- Fraud by computer manipulation
- Computer forgery
- Mutilation to or alteration of computer data or programs
- Unlawful access to computer systems and services
- Unlawful reproduction of lawfully protected computer programs.

3.2 Classification of Cyber Offences

The consensus to the classification of cyber offences by IT chief executive officers in most organisations are:

- Violations related to confidentiality, integrity and availability of computer systems and data.
  - Unlawful access
  - Unlawful interception
  - Interfering with computer data
  - Interfering with computer system
  - Mismanagement of devices
- Computer-related offences.
  - Forgery
  - Fraud
  - Child pornography
- Offences relating to copyright infringements.

3.3 Classification of Threats

The consensus to the classification of cyber threats according to the G8 countries are:

- Computer infrastructure attack
  - Denial-of-service
  - Unlawful access
  - Information mutilation in computers and network
  - Malicious acts
  - Theft of service
- Computer-assisted threat
  - Malicious activities
    - Information gathering
    - Intellectual property rights Infringement
    - Money laundering
    - Unlawful copy of data
    - Child pornography
    - Deceptions
    - Fraud
    - Drugs
    - Trafficking

3.4 Transnational Crime and Cybercrime Prevention

Crimes that have a potential effect on more than one country or offend the fundamental values of the international community are categories as a transnational crime. These crimes are said to be transnational if:

- it took place two or more countries.
- It is committed in one country, however a significant part of its preparation and planning took place in some other country or countries.
- It is committed in one country but with the help of some criminals in another country.
- It is committed in one country, however the significant effect is felt in another country.

This has clearly shown us the transnational nature of the crime which justifies the calls for international law.

Nations need some critical elements for them to be able to combat cybercrime. These elements are:

i. Responsibility and reliability of service providers

Internet and telecommunication service provider's cooperation is needed in providing internet protocol (IP) and media access control (MAC) addresses and, the location of where calls emanated. This will help in fast-tracking cybercrime prevention.

ii. Criminalisation

A distinction should be created between national criminal and international cybercrime law. The international criminal law should take off from where the national criminal law stops else some offences will have global effect only thereby freeing offenders of cybercrime in their country.

An analysis of criminalisation acts by UN shows that main cybercrime acts against the confidentiality, integrity and availability of computer systems are criminalised in many countries using cyber-specific offences. Those relating to the computer such as breach of privacy, fraud or forgery, and identity offences are often criminalised using general offences.

iii. Procedural power

An effective and efficient crime investigation is only possible with investigative powers. These powers must be regulated by law. Powers relating to gathering of electronically stored, identification and localisation of computer devices, freezing of volatile computer data and covert online investigations are needed.

iv. Electronics evidence

Parts of the evidence for cybercrime are digital in nature. Digital forensic analysis can recover volatile and contaminated information are already damaged intentionally or accidentally. Techniques like the creation of 'bit-for-bit' copies of stored and deleted information, write-protection, and file decryption 'hashes' can recover damaged information.

v. Jurisdiction and International cooperation

Three treaties have been signed that aid the collaboration of member nations in fast-tracking fighting international cybercrime. They are the extradition treaty, mutual legal assistance and the informal agency-to-agency communication.

The UN guidelines on crime have detailed all avenues that can be adopted in combating cybercrime and crime generally. It highlights that leadership in government plays a significant part in preventing crime, combined with collaboration across ministries and between authorities, non-governmental organisations, the private sector and individuals. In summary, the principles of crime prevention entail good leadership, cooperation among nations and the rule of law.

To successfully prevent cybercrime, then the underlying factors driving such crime and possible cases of victimisation must be addressed. These factors are shown in Figure 3.1.

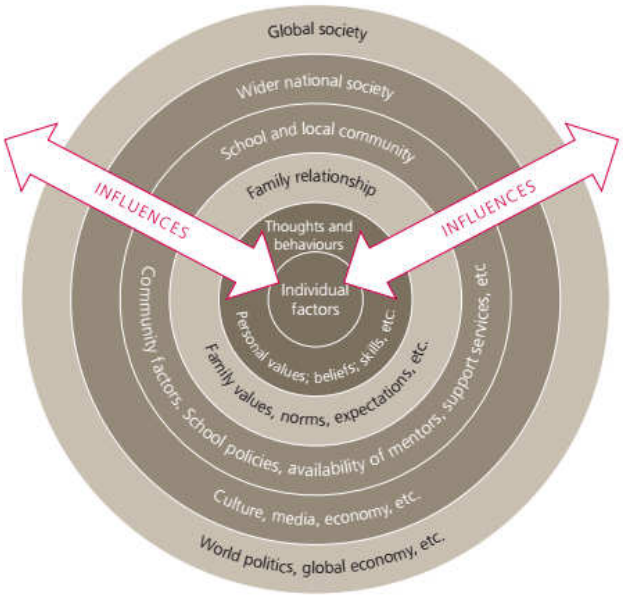


Fig. 3.1: Factors Influencing the Risks of Crime And Violence (Shaw, 2010)

Discussion

Explain how family values, norms and expectations could influence crime and violence.

Prevention methods are in-exhaustive because the crime keeps taking many dimension on a regular base. The primary prevention approaches are:

1. Crime prevention through social development.
   These are social, educational and health programmes designed for kids at young and adult age from both privileged and less privileged. These programmes help to create skills among children and give them awareness and resilience as they grow up. According to the UN guidelines on crime prevention, promoting the wellbeing of people helps in crime prevention. And also by encouraging behaviour through social, economic, health and educational measures, with emphasis on non-adult, and on the risk and protective aspects associated with crime and victimisation.
2. Locally-based crime prevention.
   Areas prone to crime due to economic factor, crimes, depression, lack of infrastructure and victimisation are targeted for crime prevention. These conditions that allow crime to bread can be worked on positively by providing adequate capital project infrastructure, better living condition, revamp businesses and the general living condition.
3. Situational crime prevention.
   Methodologies that aim to reduce or eliminate chances for people to commit crimes, upsurge the risks of being caught, and to minimise the benefits of the crime are being put in place. Installation of CCTV cameras will discourage people from committing a crime, knowing full well that they will easily be caught.

What are the necessary key constituents for developing an efficient and effective strategies for crime prevention?

Those key constituents are:

- Government's role at all levels.
- Knowledge-based crime prevention.
- Planning, monitoring and evaluation.
- Multisector methods and working in partnerships.
- Engaging communities and civil society, private sector inclusive.

4.0 Self-Assessment Exercises

1. The categories of cybercrime include the following: (select only two)
   a) Money laundering
   b) Fraud by computer manipulation
   c) Child pornography
   d) Computer forgery

Answer: b and d

2. List some factors that aid cybercrime.

Answer:
Individual factor, world politics

5.0 Conclusion

Combatting international cybercrime starts from knowing the type of offences that fall under the category. The offences need to be classified, and only then can the required prevention measure be implemented. The UN ITU through the UN Office on Drugs and Crime (UNODC) came up with guidelines on crime prevention.

6.0 Summary

Cybercrimes are crimes that are committed using a computer/network/hardware devices. These crimes are transnational and have a potential effect on more than one country, and as such, they are an international crime that requires international laws to combat them. The ITU is the UN specialised agency for information and communication technologies covering three main areas of activities: radiocommunications, standardisation and development.

7.0 References/Further Reading

Willems, E. (2019). *Cyberdanger: Understanding and Guarding Against Cybercrime.* Springer.

World Bank; United Nations. (2017). *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies (English).* Washington, D.C.: World Bank Group.

Viano, E. C. (2017). *Cybercrime, Organised Crime, and Societal Responses*. Springer.

Kremling, J. & Parker, A. M. (2017). *Cyberspace, Cybersecurity, and Cybercrime.* SAGE Publications.

Shaw, M. (2010). *Handbook on the crime prevention guidelines: Making them work*: United Nations Publications.

Unit 2: Council of Europe-Budapest Convention on Cybercrime

Contents

1.0 Introduction

In this unit, the treaty for the Council of Europe-Budapest (CoE) Convention on Cybercrime will be discussed. The treaties on cross-border crime are categorised into both domestic and international laws.

On July 1, 2004, the convention on cybercrime entered into force, but was first signed by 26 member countries in 2001. Its status as of 22nd January 2009, is that it is ratified by 23 states out of the 46 states that have signed in. This includes the United States of America (US) as a non-member state of the CoE, where it became active on 1st January 2007, and the Netherlands on 1st March 2007.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe the scope of the convention on cybercrime
- explain the jurisdiction in cybercrime
- discuss the rules of international cooperation.

3.0 Council of Europe-Budapest Convention on Cybercrime

3.1 Scope of the Cybercrime Convention

The Europe-Budapest convention categorised cross-border crime under three main scopes.

3.1.1 Substantive Criminal Law (Domestic Laws for Criminal Offences)

These are crimes that have a bearing on the availability, integrity and confidentiality of computer systems and data. These crimes are in three categories;

Computer integrity (misuse of devices, system and data interference, illegal interception, illegal access (hacking)).

Example: Illegal access (hacking)
The CoE Convention on Cybercrime had a provision on unlawful access to protecting the integrity of computer systems data by criminalising illicit access to a system. The provision in Article 2 explains that:

Countries shall approve lawful measures for criminal offences under its national law when offences are committed intentionally using any form of a computer system without right. The said country may define the offence as infringing on security procedures, with the resolved of obtaining computer data illegally or other deceitful intent pertaining to a computer system that is linked to another computer system.

Example: Illegal interception
The CoE Convention on Cybercrime had a policy for protection of the integrity of non-public transmissions of data by criminalising its unlawful interception. The provision in Article 3 explains that:

Countries shall approve lawful measures for criminal offences under its national law when offences are committed intentionally using any form of a computer system without right for the non-publicly transmission of computer data. The said country may define the offence as infringing on security procedures, with the resolved of obtaining computer data illegally or other deceitful intent pertaining to a computer system that is linked to another computer system.

Those of misuse of devices, system and data interference can be found in some references of this unit.

i. Computer-assisted
   - Forgery: The crime convention criminalises forgery under Article 7 as intentional and unlawful. It states that: mutilation of computer data thereby making it non-original with the intent of using it for legally as if it were original, regardless whether the data is directly readable or understandable is termed forgery.
   - Fraud: The convention under its fraud Act of 2006 explains that any act that results in loss of property to any person with dishonest intent is a fraud.
     i. Content related (child pornography, racism and online grooming).

Example: Child pornography

Safegauring children against sexual exploitation, the CoE convention provides an article that addresses child pornography. The provision in Article 9 explains that:

1. Countries shall approve lawful measures for criminal offences under its national law when offences are committed intentionally without right, the following misconducts:
a) distributing created child pornography through a computer system;
b) making child pornography available through a computer system;
c) acquiring for oneself or another child pornography through a computer system;
d) storing on a computer system or an electronic storage medium, child pornography files.
2. "child pornography" from item 1, is that material that portrays:
a) a child involved in a sexual act;
b) an individual seeming to be a child that is involved in a sexual act;
c) realistic images representing a child that is involved in a sexual act.
3. the term 'child' in 2 means persons below the age of 18 years.
Countries may, however, be compel to use a lower age-limit, which shall not be less than 16 years.
4. Each country may reserve the right not to apply, in whole or in part, 1c and d, 2b and c.

Those of racism and online grooming can be found in some references of this unit.

3.1.2 Procedural Law (Domestic Laws on Procedural Powers)

This is the treaty that borders on procedural power necessary to detect, investigate and prosecute cybercrime. The powers with their Article numbers are;

- Article 15 – Conditions and safeguards. This is needed to safeguard human rights and freedoms.
- Article 16 – Accelerated safeguarding of stored computer data.
- Article 17 – Accelerated safeguarding and partial disclosure of traffic data.
- Article 18 – Production order
- Article 19 - Search and confiscation of stored computer data.
- Article 20 – Collection of traffic data in real-time
- Article 21 – Interception of content data

3.1.3 Jurisdiction in Cybercrime

The territorial limits within which authority to an offender or place of offence is exercise are:

- Place - is a primary constitutive factor for jurisdiction.
- Indirect links – jurisdiction are claimed by some countries based on indirect links with their territory.
- Offender's Nationality – this is the second key constituting factor of the domain in cybercrime.

3.2 Rules of International Cooperation.

The 2001 Budapest convention is targeted as the most successful treaties in fighting cross-border cybercrime because of the involvement of even the non-member states. The convention combines the four aspects of cybercrime (that is, the substantive, procedural, jurisdictional and international cooperation) and makes it binding on all member states. The provision of making member states safeguard human rights and freedom while fighting cybercrime makes it indeed a global instrument.

The provision for extraditing a target is contained in the Convention. However, the requirement to extradite is restricted to offences established by the Convention, the principle of dual criminality and to offences punishable by the denial of freedom for at least a year or by a penalty that is more severe.

Discussion

Discuss the four primary waves of national legislation between 1970 and 1990

4.0 Self-Assessment Exercise

1. Mention citing examples in each case, three categories of computer crime or cybercrime.

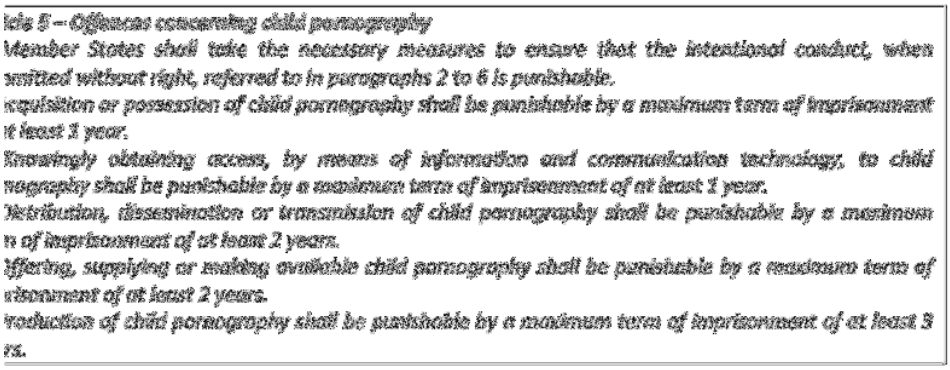
   Answer

   (a)The use of a computer systems as a target of criminal activities (for example, dissemination of viruses, hacking). (b) The use of a computer systems as tools or instrument to commit a criminal activities (for example, online fraud). (c) The use of a computer systems as incidental to a crime (for example, data storage for criminal activity).

2. What Article in the COE Convention covers the protection of a child against sexual abuse and exploitation?

   Answers

   Article 5


Article 5 – Offences concerning child pornography
Member States shall take the necessary measures to ensure that the intentional conduct, when committed without right, referred to in paragraphs 2 to 6 is punishable.
Acquisition or possession of child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.
Knowingly obtaining access, by means of information and communication technology, to child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.
Distribution, dissemination or transmission of child pornography shall be punishable by a maximum term of imprisonment of at least 2 years.
Offering, supplying or making available child pornography shall be punishable by a maximum term of imprisonment of at least 2 years.
Production of child pornography shall be punishable by a maximum term of imprisonment of at least 3 years.

5.0 Conclusion

The CoE is the most detailed and influential cyber-specific instrument which for example addresses most crucial issues in the area of cybercrime. Also, its binding nature on countries involved has increased its effectiveness and suits its ambition in harmonisation them. Moreover, the indirect effect of the Convention has undeniably been far-reaching, serving as a exemplary for legislation, offering a wide range of guidance and generating considerable debate all over the world. The Convention further enhanced

international cooperation, even among countries with already existing relations.

6.0 Summary

In 2001, 26 member countries convened in Budapest and signed the CoE Convention on Cybercrime because of the rising number of certain computer-related offences which requires special attention. The convention became active force on July 1, 2004. The treaties on cross-border crime are categorised into both domestic and international laws.

7.0 References/Further Reading

Kremling, J. & Parker, A. M. (2017). *Cyberspace, Cybersecurity, and Cybercrime*. Sage Publications. Retrieved from https://dl.acm.org/doi/book/10.5555/3180792.

Shaw, M. (2010). *Handbook on the Crime Prevention Guidelines: Making Them Work.* United Nations Publications. Retrieved from https://www.unodc.org/pdf/criminal_justice/Handbook_on_Crime_Prevention_Guidelines_-_Making_them_work.pdf

Module 4: Dispute in Cyberspace

Module Introduction

Intellectual property (IP) is the creation of the mind, which is unique in every sense when adequately harnessed. Novelty and the creation of new works and products can only be sustained if laws are guiding the output of those ideas. IP laws protect ownership of ideas that have been disclosed. The world has been relatively succeeded at establishing blockades to prevent acts that would undermine innovation, in the form of copyright, trademark, design right and patent regulations. This enabled IP inventors to use their inventions as they so wish or release it without fear of losing control over its use. It is presumed that IP right helps in motivating creativity and ingenious activity and make for orderly marketing of patented goods and services. But with the introduction of the internet, plagiarism has become easy and enhanced that widespread abuse of IP right is common thereby affecting the rights of the IP owners.

Internet-related crimes are numerous and cutting across all phases of life. When IP rights are being infringed over the internet, where the victim and perpetrator are of different country origin, then jurisdictional issues arise. Jurisdiction of a state to criminalise any act has traditionally been based on its sovereign control over that specific territory in question which is known as the principle of territoriality. With such a control, the state is theoretically in a position to exert jurisdiction in its fullest extent for crimes occurring between people in that space and to do so to the exclusion of all other powers.

Unit 1: Intellectual Property Issues
Unit 2: Jurisdiction and International Law

Unit 1: Intellectual Property Issues

Contents

5.0 Conclusion
6.0 Summary
7.0 References/Further Reading

1.0 Introduction

In this unit, cybercrime-related to issues of intellectual property (IP) will be discussed. Some of the rights as regards invention and ideas will also be treated. IP is an idea and invention developed by a person. This could be in the usual course of an employee's duties, which then belongs to the employer, unless entirely unrelated to the employee's usual work. It is therefore advisable to specify what inventions might fall within the course of their regular duties in employees' contracts. They will, however, retain a right to claim a fair share of the benefits of their invention.

Protection varies but aims principally at stopping competitors or fraudsters exploiting your product or process without permission. This protection covers laws relating to copyright, trademarks, patent, design right, protection against competitors and commercial exploitation of industrial secrets.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the significance of the Internet on IP
- discuss copyright protection in cyberspace
- investigate cybercrime related to copyright, trademark, patent etc.

3.0 Main Content

3.1 Significant of the Internet on IP

The Internet has played a substantial role in technological development. It has made access to ideas and solutions to questions easy. The Internet, as a resource tool, has made access to resources quite easier. Goods are sold, and services are provided using the internet. Businesses have flourished even though some are not legitimate due to right infringement. These rights infringement raises several issues for IP in addition to those that would come up in respect to products. Some of the impacts the internet has made on IPs are as follows:

- It has globally increased access to IP resources.
- It has enhanced the ability of patent earlier art search.
- It has increased awareness of the need for IP.
- It has shortened information and data access time as regards IP rights.
- It has increased the volume of avalable data and collections relating to IP.
- It has provided access to IP web-based software and management tools.

An example of the negative effects the internet has caused the IP rights is:

- It has made worse the 'poor patent quality'. This has negatively affected shareholder value, IP value and the overall economy.

3.2 Copyright Protection in Cyberspace

Copyright law gives an author or inventor the exclusive right to make copies of their work and encourages them to exploit their work commercially though for a precised period. Copyright protection covers a vast area of protection (for example, literary, artistic and musical works, computer programs and databases, films, recordings, broadcasts and cable programmes).

Technology has some negative effected on the copyright law because of the software tools and hardware gadgets that are used to pirate inventions. Before digitisation, the quality of a copied videotapes is lost. The IP law tackles violation of the exchange of copyright-protected software, files and songs. The content scrambling systems (CSS) is used by the entertainment industry to prevent the mass copying of CDs and DVDs. The digital rights management (DRM) allow copyright-holders the restriction to allow customers the right to air their music (audio or video) for a specific period. This law also extends to TV stations, but the use of hardware devices has made it possible for offenders to crack channel encryption code to watch channels of their choice.

3.3 Patent

While copyright protection relates to literary works, the patents protect 'uniqueness' of technological inventions covering both processes in physical production and physical products. The patent is a grant by the government to the inventor for the production and sale of the invention for 20 years, starting from the date of application. Renewal is, however, allowed. The eligibility for application of patent is the novelty and economic benefit of the invention (process, the machine, and composition of matter).

Patent protection outside one's country is obtained by applying to that country of interest or an application under the year 2000 European Patent Convention (EPC) or the Patent Cooperation Treaty (PCT) of 1970 as

amended. The world IP organisation (WIPO) administers the the PCT. The time duration for PCT is shown in Figure 4.1, and other details can be gotten from the PCT application guide.

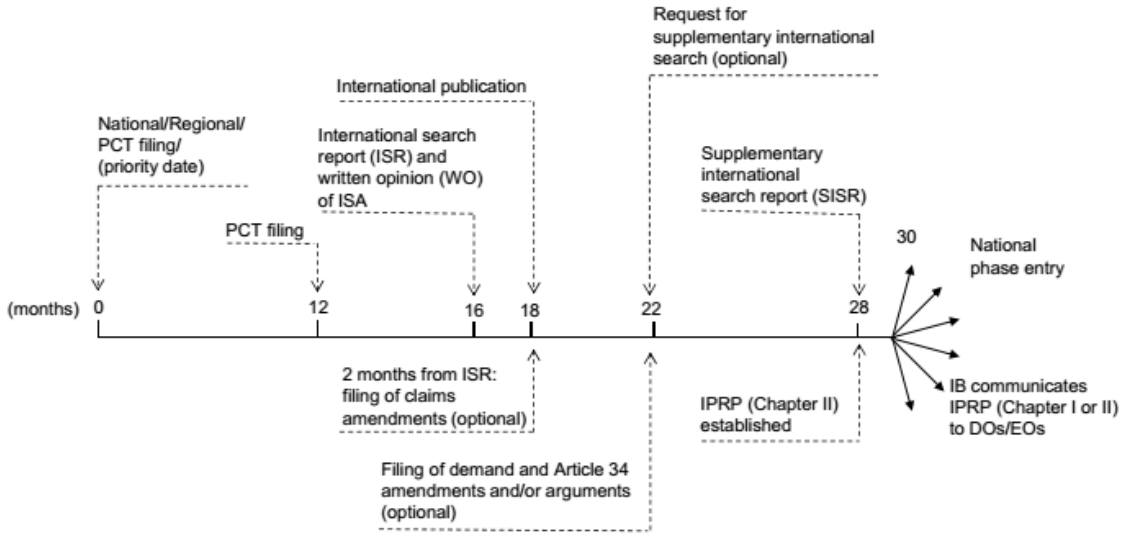


Fig. 4.1: PCT Timeline (Mishra, Akash kamal, 2019)

3.4 Trademark

A trademark refers to the protection of commercial labels on the internet, which is subject to renewal every ten years. As is the case for patents, only filed and granted trademarks after an examination process by the relevant authorities are protected by law. Trademark violations being similar to copyright violations are part of cybercrime now which have a varying degree of criminalization under the national penal code. Criminal activities in trademark happen with the use of other people's businesses domain name, thereby misleading others into believing the offender is the owner of the business. Domain name availability can be checked online to make sure they have not been taken.

3.5 Design Right

This is the protection of the appearance of mass-produced articles. It is an infringement for articles to be copied 'exactly or substantially' from the original design. Importing, possessing for profitable purposes, or dealing commercially with an infringible article, is a secondary infringement. For example, Michelin tyre company has the right to protect the treads design of its tyres from other competitors.

Other forms of IP rights are protection against competitors using other people's products as yours, commercial exploitation of industrial secrets and service marks.

 ..Discussion

What are the ownership protections provided by law as it relates to the legal requirements of intellectual property?

4.0 Self-Assessment Exercise(s)

1. Give one example each on the positive and negative impacts the internet has had on IP that were not mentioned earlier.

   Answer
   Positive impact
   - Provided a path for breaching IP knowledge between the developing and the developed world nations.
     A negative effect the internet has caused on the IP right is;
   - It has produced new IP problems, infringement possibilities and enforcement challenges, such as cybersquatting, trademark infringement etc.

2. What are the basic requirements for the patentability of an invention?

   Answer
   - The novelty of the invention.
   - The steps of actualising the invention.
   - The capability of industrial application, and not being part of what is excluded as an invention.

5.0 Conclusion

The relationship of all the IP rights to the recent technology that exploits their vulnerability is seen as retarding progress. Generally, courts decline to find infringement when copyright owners seek to eliminate a new kind of dissemination that the court deems not harmful to copyright owners. Though, when IP owners agree instead to receive payment for the new modes of exploitation, the courts and law-making bodies then enforce copyright control over that new market. Nowadays, the IP legislative bodies

regard the unlawful distribution of works over the internet as preventing copyright owners the ability sell their work through the digital market.

6.0 Summary

Some of the impacts the internet has made on IP both positively and negatively are:

- It increased access to IP resources globally.
- It enhanced the ability of patent prior art search.
- It increased awareness of the need for IP rights.
- It shortened information and data access time as regards IP rights.
- It has made worse the 'poor patent quality'. This has negatively affected shareholder value, IP value and the overall economy.
- It has produced new IP problems, possibilities infringement and challenges in enforcement.

Protection varies but aims principally at stopping competitors exploiting owners product or process without consent, and it covers the following areas:

- patent law – protection of the novelty in technological inventions;
- copyright – protecting literary, artistic and musical works, computer programs and databases, films, recordings, broadcasts and cable programmes;
- design right – protection of the appearance of mass-produced articles;
- trademarks –commercial labels protection;
- protection against competitors disparaging your products maliciously and 'passing off' their products as yours;
- commercial exploitation of industrial secrets.

7.0 References/Further Reading

Willems, E. (2019). *Cyberdanger: Understanding and Guarding Against Cybercrime. Springer*. Retrieved from https://www.springer.com/gp/book/9783030045302

Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Unit 2: Jurisdiction and International Law

Contents

1.0 Introduction

In this unit, the principle of territoriality, the principle of active and passive nationality based on the Council of Europe (CoE) Convention on Cybercrime, will be discussed. Other principles that will be covered are the protective principle and the principle of universality.

The jurisdiction of a state to criminalise an act has conventionally been based on its supreme control over that particular territory in question which is known as the principle of territoriality. With such a control, jurisdiction by states are theoretically exerted to the fullest for crimes occurring between people in that space and to do so to the exclusion of all other powers.

Cybercrime being transnational involves different jurisdiction. The global information infrastructure is expanding in geometric order and so also is the cybercrime. The obstacle face by nations in solving cross-border crime is due to the jurisdictional law of states. Cybercrime can be committed by an offender in country A using internet services in country B while the effect of the crime is felt in countries C, D or E. This will pose serious challenge in the application of criminal law and leading to questions about state jurisdiction, which country will lead the investigation and how the disputes will be resolved.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the principles of territoriality
- state the principles of active nationality
- discuss the principles of passive nationality
- explain protective principles.

3.0 Main Content

3.1 Principle of Territoriality

The conventional understanding of jurisdiction operates on the premise that the states have inherent authority over crimes occurring in its territory. It should be ideal that the affected state where the crime by the offender is committed has the jurisdiction over the trial of such crime. The Europe Council on Cybercrime in its Article 22 paragraph 1a explains that:

Article 22 – Jurisdiction

1. Countries shall approve lawful measures to establish jurisdiction for criminal offences under Articles 2 through 11 of the CoE when the offence is committed either:
   a. in its State.
   b. on a ship flying the contries flag.
   c. on an airplane duly registered with that country.
   d. by a citizen in that country, for an offence punishable under the country's criminal law; or for offences committed outside the jurisdiction of that State.

From this Article 22, the example given in the introduction means that countries C, D, E has the sole jurisdiction of the trial base on item 1a. The case still becomes complex because each of the countries C, D and E has jurisdiction to try the case though independently.

3.1 Principle of Active Nationality

The principle of nationality refers to a jurisdiction that is exercised concerning the actions of nationals outside their countries. It is associated with the power a country has in regulating the behaviour of its nationals both outside and within the country. This is a principle that is common in countries that practice civil law. Since offenders can commit Internet-related crimes without them leaving their country, the policy is of less

significant when it pertains to cases of cybercrime. However, it can be very applicable in the perspective of production of child pornography for the sole aim of distributing it through computer networks. An example of such an approach is the paragraph 1d of Article 22 of the CoE Convention on Cybercrime.

Article 22 – Jurisdiction
1. Countries shall approve lawful measures to establish jurisdiction for criminal offences under Articles 2 through 11 of the CoE when the offence is committed either:
   a. in its State.
   b. on a ship flying the contries flag.
   c. on an airplane duly registered with that country.
   d. by a citizen in that country, for an offence punishable under the country's criminal law; or for offences committed outside the jurisdiction of that State.

3.2 Principle of Passive Nationality

While the principle of active nationality applies to offenders concerning their nationality, that of passive nationality applies to a victim of a perpetrated crime. The passive nationality principle denotes to jurisdiction on the grounds of the victim's nationality. The principle applies if a citizen becomes a victim to a crime while outside their country. Controversial application of this principle is discussed because it specifies that foreign law is sometimes inadequate to protect foreigners. Section 7 is an example of a non-Internet-specific code of law formulation for the principle of passive nationality in the German Penal Code. This section states that;

Section 7
For cross-border;
1. Criminal law in Germany shall apply to crimes committed overseas against its citizen, if the act is an offence within its locality or for localities not subjected to any criminal jurisdiction.

3.3 Protective Principle

The protective principle just like the 'effect doctrine' is triggered when a crime caused by an action outside the country it happened affects not just a national (the victim) of the state, but also affects national security interest be it domestic or international: for instance, the proper functioning of the government. The protective principle is contentiously discussed because the offender, victim and the infrastructure used are all absent.

3.4 Principle of Universality

This principle establishes jurisdiction for some specific crime and requires an international or consensus agreement. A sovereign's right to adopt criminal laws restricting the conduct is recognised by the principle, regardless of who commits it, or where it was committed, so long as restricting that conduct is recognised by countries as being of international concern. A classic example of international crime is piracy on the high seas. However, countries that have adopted this principle went further to develop it. Section 6(6) of the German Penal Code with a provision that can be applicable to cybercrime cases is a classical example. This is used for offences committed outside of Germany against internationally protected legal interests.

For the following offences committed overseas, the criminal law in Germany will further apply, irrespective of the criminal law of the crime host country:

1. revoke;
2. crimes concerning the use of nuclear material under sections 307, 308(1) to (4), 309(2) and 310;
3. maritime and air attacks (section 316c);
4. sexual and work exploitation using human trafficking (Sections 232 to 233a);
5. illegal drug dealing;
6. pornography distribution under the following sections: 184a, 184b(1) to (3) and section 184c(1) to (3), also in connection with part of section 184d.

3.5 National Frameworks

Even though international instruments are used to solve the problem associated with cross-border crime jurisdiction, national (country) legal framework is needed to ease cooperation among nations. This framework can be implemented either formally or informally. The formal way is all the processes (sections 3.1 through to 3.5 of this unit) that are above. In the informal approach, jurisdictional issues on a case-by-case basis will be address by nations and authorities through informal understandings that were based on trust and shared experiences of cooperation enjoyed over time.

3.5 Convention against Transnational Organised Crime

The United Nations (UN) serves as the main international instrument for international cooperation in the fight against cross-border crime. The Article 2 of the UN Convention on Transnational Organised Crime (UNTOC) have

detailed what organised criminal groups are. Mutual legal assistance between states is defined in detail in Article 18 (section 1-30) of the UNTOC. Articles 23, 24 and 25 deals with the general principle of international cooperation, extradition and the general principle of mutual assistance, respectively.

 Discussion

A cybercrime was committed by an offender in Germany using internet services in America while the effect of the crime is felt in Nigeria. By using Article 22 of the CoE Convention on Cybercrime, state, with reasons, which of the countries has jurisdiction over the crime.

4.0 Self-Assessment Exercise(s)

1. Using Article 22 of Jurisdiction, explain the "flag principle" as it relates to cybercrime jurisdiction.

   Answer

   The flag principle is related to the principleof territoriality but incorporates domestic laws on ships and aircraft. Internet access solutions availability in maritime and air transportation questions the use of criminal law for cases where either the offender, victim or even the computer systems being used are all not in the territory where the crime took place but rather outside the territorial borders of the country.

2. Which Article in the UNTOC is related to the general principle of mutual assistance?

   Answer:
   Article 26 and it states that.

> *Article 26 – Spontaneous information*
> *1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.*

Mini project
Write a phishing email pretending it is from Amazon to a person who has an Amazon account requiring them to update their Amazon.com account information such that they will give away their account login details.

5.0 Conclusion

The development of national legal frameworks by countries will enhance solving transnational cybercrimes. These frameworks allow states to create means of investigating and prosecuting offences which are targeted at them, affect them and, which were lunch within or outside their border. The formal approach to the framework from various Article sections and paragraphs in the CoE Convention on Cybercrime has addressed all the current issues raise. However, they need updating due to the nature of new cross-border crimes.

6.0 Summary

The following principles are examples of adaptive jurisdiction principle: the principle of territoriality, the principle of active nationality, passive protective principle and the principle of universality. These jurisdictional frameworks can be implemented either formally or informally. The CoE Convention on Cybercrime has addressed all the current issues raise though they need updating due to the nature of new cross-border crimes.

7.0 References/Further Reading

Peterson, D. S. & Das, D. K. (2017). *Global Perspectives on Crime Prevention and Community Resilience:* CRC Press. Retrieved from http://publichealthinsurance.xyz/booker/oiy8dwaaqbaj/

World Bank; United Nations. (2017). *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies (English).* Washington, D.C.: World Bank Group. Retrieved from http://documents.worldbank.org/curated/en/355401535144740611/Combatting-Cybercrime-Tools-and-Capacity-Building-for-Emerging-Economies

Module 5: Cyber Ethics and Emerging Trends

Module Introduction

Cybersecurity practices aim at securing computer and network (software and hardware) data. Aside from the values that the data has, cybersecurity entails the protection of information confidentiality, integrity, availability, and the human and institutions that use the information. In protecting those organisations and their data, cybersecurity professionals inversely safeguard the lives and happiness of all humanity that have links to the information being protected.

For instance, if a cybersecurity expert is responsible for securing a health facility's network and critical data from cyber attack, then the person is indirectly involved in protecting all sick patients that are attached to that health facility. Those patients' health and privacy are now linked to the cybersecurity expert's success or failure in securing the network. Cybersecurity profession and their personnel have the responsibility of information relating to credit card, schools, power and water customers, airline, inventors etc.

Ethical issues have always been a core practice of the cybersecurity profession because the practices are required for securing and shielding individuals and organisations to live well.

Unit 1: Ethical Concepts and Professionalism
Unit 2: Emerging Trends in Cyber Laws and Ethics

Unit 1: Ethical Concepts and Professionalism

Contents

1.0 Introduction

In this unit, the essential ethical issues in cybersecurity are discussed. You will know the everyday ethical challenges cybersecurity professionals face and also study the general ethical framework that guides cybersecurity practice. The unit will conclude by outlining the ethical best practices in cybersecurity.

Ethics is that system of moral principles that relates to the benefits and ills of some actions, and to the appropriateness and injustice of motives and ends of those actions. Cybersecurity aims at securing computer and network security data from being damaged and stolen.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain critical ethical issues in cybersecurity
- discuss ethical challenges for cybersecurity professionals
- describe best practices for cybersecurity ethics.

3.0 Main Content

3.1 Important Ethical Issues in Cybersecurity

Practices in cybersecurity can significantly impact the fundamental interests of human beings. Design choices in building that are unethical, for example, can have negative impact on human integrity and harm human health, and with this makes it difficult for people to thrive. Unethical decisions in cybersecurity could have negative impacts on reputation and earnings. Good cybersecurity practices has so many advantages the society can benefits from which include safer infrastructure. This can further reduced social and economic anxiety, and increased investment and invention.

3.1.1 Harms to Privacy

Some of the cyber threats lead to infringement on privacy. Hacking among so many other intrusions in networks and the internet are used to obtain sensitive information about individuals and corporation. Illegal access of individual's sensitive information can be used to blackmail, extort and commit so many other forms of crime. Violation of individual's privacy of this nature are sometimes on victims to harm the interests of third parties. For example, blackmail can be used to pressure a compromised employees (victim) to give away confidential client information, business secrets, or even bring an end to a competitor's business.

3.1.2 Harms to Property

Harms can be caused by cyber intrusion into an individual or organisations data bank and stealing funds, inventions (intellectual property), trade secrets, passwords, and even corrupting or destroying information. This could be because of individual, political or market competition. Unauthorised harm to a property through cyber intrusion is unethical, and this can lead to not only damaging the property but harming individuals as well. Harms to some property can be justified, especially if it is for national interest and the targeted group or individuals are wanted criminals.

3.1.3 Resource Allocation

Securing information is essential but when too many resources are allocated to such service, then it becomes even more expensive to sustain it. Cybersecurity consumes individual and organisations resources in terms of time, money, and expertise. If the resources needed to maintain or continuously prevent cyber attacks is not sustainable anymore, then a balance must be reached else, the whole effort will be compromised.

3.1.4 Transparency and Disclosure

Transparency in organisational practice to client and disclosure of risk vulnerability, especially when it will have a direct impact on the client is an important ethical issue. Since cybersecurity is a form of risk management which could significantly affect other parties (people or organisation), then it is ethically right to make those risk vulnerability areas to be known, so that informed decisions can be made by those affected. For example, customers/clients should be notified of any critical vulnerability in a particular software by the company on time so that patches can be installed once available as a defensive measure.

Case Study

Mike is a cybersecurity consultant approached by a new startup company, BioHak, which plans to develop a revolutionary but controversial new consumer product: a subdermal implant that will broadcast customers' personally identifying information within a 10-foot range, using strong encryption that can only be read and decrypted by intended receivers using special BioHak designed mobile scanning devices. Users will be able to choose what kind of information they broadcast, but two primary applications will be developed and marketed initially: the first will broadcast credit card data enabling the user to make purchases with the wave of a hand. The second will broadcast medical data that can notify emergency first responders of the users' allergies, medical conditions, and current medications. The proprietary techniques that BioHak has developed for this device are highly advanced and must be tightly secured in order for the company's future to be viable. However, BioHak's founders tell Mike that they cannot presently afford to hire a dedicated in-house cybersecurity team, though they fully intend to put one in place before the product goes to market. They also tell Mike that their security budget is limited due to the immense costs of product design and prototype testing, so they ask him to recommend a free open-source software (FOSS) solutions for their security apparatus and seek other cost-saving measures for getting the most out of their security budget. They also tell him that they cannot afford his full consulting fee, so they offer instead to pay him a more modest fee, plus a considerable number of shares of their company stock.

Question:

i. In the sub-sections of section 3.1, what risks of ethically significant harm are involved in the case study above?
i. If Mike makes poor choices in this situation, who could be harmed and how?

3.2 Ethical Challenges for Cybersecurity Professionals

It is possible to have unethical legal cybersecurity practices. These acts can result to harm and create reputational damage to network users, individuals, organisation and cybersecurity professionals. Some of these ethical challenges are discussed briefly.

3.2.1 Balancing Security with Other Values

An ethically acceptable balance must be sort between cybersecurity the following;

1. Network and device usability, reliability, speed, and all resources needed by both the organisation and the stakeholders.
2. Clients, customers, employees and users
3. Any possible harm it is causing due to security breaches or resource allocation.
4. Privacy, consistency in services delivery and transparency in conducting the organisation security affairs.

3.2.2 Threats/Incidence Response

The organisation should have in place an appropriate response plan or strategies for the worst-case scenario of threats or incidences even before they occur. Resources should be available, and action-oriented implementation plan should be in place whenever the need arises. Ethical grey areas should be identified and resolved.

3.2.3 Security Breaches/Vulnerability

Security breaches or vulnerability answers must be available and provided for the following questions:

- Does a viable plan in the organisation exist for how and when to notify network or software users on breaches and vulnerability as it relates to security incidents?
- How can accurate, timely, and helpful reporting of security incidences be meet by the organisation?
- Has the organisation considered not only their perspective but the view of other stakeholders?
- Have they identified an ethical balance on reacting to security breaches and vulnerabilities?

3.2.4 Network Monitoring and User Privacy

Continuous monitoring of the network is essential to know when it is secure and when a breach occurs. That way, security hacks will quickly be noticed and averted. Responses to ethical issues relating to network monitoring and privacy should be available. Some of those moral questions that need answering are:

1. How can unjustifiable intrusions upon users and their privacy be avoided while making an effecting network monitoring?
2. Can the network activities of personal devices (laptops, tablets and cell phones) not owned by our organisation and lawfully used for many other purposes be monitor and control?
3. To what degree do users need to know of our security monitoring activities?

3.2.5 Competing Interest and Obligation

Questions regarding ethical challenges with competing and obligation should be asked. Some of the questions are:

1. For both short-term and long-term cases, what are the are the extend of the ethical harms that may result due to security breaches and to whom?
2. What should we do in granting someone a level a system access privilege that is authorised by an employer or client knowing fully well that it is inappropriate?
3. What should we do in putting off disclosure of critical system vulnerability that authorised by an employer or client?
4. In the event that we are asked to violate a professional cybersecurity practice in the interests of national security, what do we do?
5. Between myself and those I am professionally bound to protect regarding cybersecurity services, what sorts of compensation arrangements do I think might create a conflict of interest?

Other ethical challenges in which each has its individual questions that need answering has to do with:

a. Data storage and encryption
b. IoT, smart grid and product design
c. Accountability for cybersecurity
d. Security research and testing
e. Impacts of cybersecurity practices

3.3 Ethical Framework Guide to Practicing Cybersecurity

Aside from the professional obligation, that cybersecurity personnel of an organisation has to the public, those to fellow humans are equally important and could affect the cyber world.

3.3.1 Virtues Ethics

Virtue ethics can help in determining and understanding our moral obligation. Firstly, there is that need to develop once moral character by consistently making an effort in knowing what is required and make amends

where wrongs have been done. Secondly, is where exactly to look in getting the standard of those ethical conduct that is worth emulating. These are sort for in the society we live from those unique exemplary individuals that are known to be of good moral character. Thirdly, the virtues ethics guides one toward application of learned practical wisdom and good moral judgment.

 Discussion

What aspect of your characters do you need to improve on to become a better person?

3.3.2 Consequentialist/Unilaterian Ethics

Consequentialist principles of ethics guide moral action aginst the likely consequences of those actions. If the consequence of an action by one will be perceived negatively by all, then those activities are morally wrong and should be avoided. The principle of using the greatest good to decide in a given situation what our moral obligation are is a unilitarian ethics is a form of consequentialism.

3.3.3 Deontological Ethics

These are rules of ethics, in which one or more of the principles informs us of what our moral obligations are. Take, for instance, the 'universal human rights' idea from the western that all countries are expected to agree with though these could be based on some few individual's ideologies which may not necessarily be those of the society or community. While gays are allowed in some country, it's a complete taboo in so many different culture and countries.

3.4 Best Practices for Cybersecurity Ethics

There can't be a particular exhaustive code of cybersecurity ethics that can be fitted to all scenerios in an organisation or individual pratctices. However, specific internal guidelines and best practices for cybersecurity ethics can be developed which can then be adapted to their activities and challenges. The exhaustive codes of practice can be modified while reflecting on some ethical cybersecurity practice general norms and guidelines:

1. Cybersecurity ethics should be the focus
2. Human lives and interests behind the systems should be considered
3. Consider the downstream risks in cybersecurity practice
4. Establish chains of ethical responsibility and accountability
5. Practice cybersecurity disaster planning and crisis response
6. Promote values of transparency, autonomy, and trustworthiness
7. Consider disparate interests, resources, and impacts

8. Invite diverse stakeholder input
9. Design for privacy and security
10. Model and advocate for ethical cybersecurity practice

4.0 Self-Assessment Exercise(s)

1. In monitoring security activities of the network, to what degree should users know about it?

   Answer: Network monitoring and user privacy

2. One among the following is not a possible question that will need answering in dealing with ethical challenges in encryption and data storage.
   A. How can we store and transmit sensitive information responsibly and safely?
   B. Should adequate care be taken while contracting with third parties?
   C. In term of the various forms and strengths of encryption we might use, what ethical risks and benefits associated with it?
   D. What are the competing interest and obligation?

   Answer: D

5.0 Conclusion

In demonstrating ethical concept and professionalism in cybersecurity, the importance of those ethical issues needs to be identified first. The organisation or individuals need to know ethical questions that must have answers anytime they are required. It is in answering those questions that an ethical framework that guides cybersecurity practices can be developed.

6.0 Summary

This unit started by looking at the essential ethical issues associated with cybersecurity. Concerned raised addresses issues on privacy, resource allocation, transparency in activities and those of intellectual property. Cybersecurity professionals face various ethical challenges ranging from those of data storage and encryption, IoT, smart grid and product design. Others are security breaches, network monitoring, user privacy, and lastly opposing interest and obligation.

7.0 References/Further Reading

World Bank; United Nations. (2017). *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies (English).* Washington, D.C.: World Bank Group. Retrieved from http://documents.worldbank.org/curated/en/355401535144740611/Combatting-Cybercrime-Tools-and-Capacity-Building-for-Emerging-Economies

Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* Retrieved from http://documents.worldbank.org/curated/en/355401535144740611/Combatting-Cybercrime-Tools-and-Capacity-Building-for-Emerging-Economies

Unit 2: Emerging Trends in Cyber Laws and Ethics

Contents

1.0 Introduction

In this unit, cybercrime law as an integral part of the cybersecurity strategy will be discussed. You will know what areas cybercrime policies will cover. The roles regulatory agencies play in fighting cybercrime will be covered too.

Cyberlaw entails the safe and lawful collecting, retening, processing, transmission and use of internet-related data which can include computer system hardware and software. These laws help in mitigating substantial damage from activities of cybercriminals by protecting information confidentiality, integrity and availability.

Ethics can be referred to as the moral responsibility that a person owes another. It also refers to the standard norms that are set up by some particular culture, society or race of a country. Besides, ethics refers to handling of morals by the use of the right principles as layed down by a given system of professional conduct. The application of responsible behaviour to internet-related affairs is known as cyberethics which in many cases aligns with acceptable behaviour in everyday life, though the costs can be significantly different.

While laws are governed by an organisational or government body, ethics is not. Murder, theft and assault for example are actions that deviate from legal and ethical codes throughout the world.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- review the current trends in cyber laws and ethics
- explain the role of regulators in fighting cybercrime.

3.0 Main Content

Due to the problematic and developing nature of cybercrime, cyber law has become very important and therefore gaining attention every single year. The methodologies need to be dynamic to fight these crimes. And some of the recent trends in cyber law that address those trends are:

1. New and more severe regulations.
2. Strengthening of the current/existing laws.
3. Awareness of privacy issues needs to be improved.
4. Cloud computing.
5. How virtual currency might be vulnerable to crime.
6. Usage of data analytics.

3.1 Cybercrime Legislation as a Cybersecurity Strategy

Developing technical protection systems and educating internet users can prevent them from becoming victims of cybercrime which will help in reducing the risk associated with cybercrime.

Implementation of existing strategies
Existing strategies that have worked in some countries can be introduced in others. This will save resources and allow for faster implementation of the strategy. The only challenge from the existing anti-crime strategies is that: does the adopting country has the resources and capabilities to implement them?

Other issues to be considered by the adopting countries include compatibility of the existing legal system, the extent of of self-protection measures that will be put in place and the private sector support involvement.

Regional differences
There is a need to harmonise national laws and techniques in combatting cybercrime. This should involve taking into account the regional demand and capacity of the nations.

3.2 Cybercrime Policy

Developing policies or law will help countries when it comes to responding to cybercrime problems. These new policies if not already in existence, should be included in the existing policies.

Responsibility within the government
Those aspects of cybercrime countermeasures could be interrelated to the mandate of the Ministry of Communication, Ministry of Justice, Economic and Financial Crime Commission (EFCC) for instance and more. While developing a cybercrime policy, the role of each of the various government bodies should be clearly stated.

Defining the different components
The various activities are coordinated using the developed policy regardless of which government body is implementing it in the long run. The components could be from strengthening institutional capacities (for example, the police and judiciary) to the introduction of more advanced legislation.

Determination of stakeholders
The policy should address stakeholders in addition to government institutions. It may be required in the development of guidelines with consideration for the sectors of the government, private and NGOs.

Identification of benchmarks
As a way of preventing international and local internet users from becomes cybercrime victims, higher priority should be given to methods of increasing cybercrimes prevention. There should be harmony in developing cybercrime legislation meant for local and international standards.

A cybercrime policy model explains that: Provisions shall exist for both regional and internationally accepted offences relating to cybercrime such as SPAM. Cybercrime legislation shall be made to be compatible to both regional and international best practices in order to ensure its ability for enforcement by countries in various region and the international community.

Key topics for legislation
The major aspect that should be addressed by the legislation should be included in the policy document, which should consist of an outline of offences that should be covered.

Amendments and updates of legal frameworks
The liability of an Internet Service Provider (ISP), electronic evidence, and international cooperation issues should be included in the cybercrime legislation. In many countries, legislation may already exist which might be in a different legal framework. Provisions relating to cyber offences can be implemented in separate legislation by updating older law to accommodate newly suggested ones.

This method of effecting cybercrime legislation by valuing structures in place is more challenging than merely using a regional standard or international best practice in an independent piece of legislation.

The relevance of crime prevention
Even though punishment threats most a times prevent crimes, the main aim of crime legislation is sanctioning the crimes and not in preventing it. However, preventing crimes is recognised as a significant element in the fight against cybercrime. Crime mitigation such as firewalls and anti-virus can prevent access to a computer system and hinder installation of malicious software, respectively.

3.3 The Regulator's Role in Fighting Cybercrime

Initially, legislation happens to be the main area discussed when it comes to addressing cybercrime, but the focus is now on the role of regulators in the fight against cybercrime.

Telecommunication regulation to ICT regulation
Information and Communication Technology (ICT) regulatory agencies are now fully involved in a range of activities liken to combatting cybercrime. This find its relevance in network safety, content regulation, and consumer protection. The involvement of regulators is because cybercrime has undermined advancement in the ICT industry and their capabilities. The new roles of the ICT regulator in fighting cybercrime include developing policies for consumer protection, industry development and cyber safety to implementation.

Extending the responsibility of regulators
The detail interpretation of existing mandate or creating new ones are the two primary objectives in the establishment of regulators for combating cybercrime. The two known fields that have always been the primary job of regulators are consumer protection and network safety. The focus on consumer protection has changed due to a paradigm shift to Internet-related services from the telecommunication services.

Regulator involvement in fighting cybercrime
Only a few ICT regulatory bodies have the mandate in going beyond regulation to now deal with issues in a broader perspective. Operating in

a dynamic and fast-developing environment exposes ICT regulators to new found areas that were initially known only as domain for government agencies. The regulator's likely involvement areas are outlined below:

1. Global policy strategies
2. Development of cybercrime legislation
3. Detecting and investigating cybercrime
4. Facilitation of law enforcement

Authorised measures
Legal measures, among other anti-cybercrime strategies, are the most pertinent for fighting cyber threats both locally and globally.

Substantive law: This requires provisions of the law that criminalises acts such as copyright violations, child pornography, computer fraud, illegal access and data interference. Rules that exist in the criminal code for other offences might not apply to internet committed acts. Hence, an exhaustive analysis of current national laws is important to identify any possible gaps.

Procedural law: Apart from provisions provided by substantive law, agencies that enforce law need the required resources to investigate cybercrime. Offenders can act from anywhere in the globe while hiding their identity. The resouces required in investiging cybercrime might be utterly different from those used to investiging common crimes.

Electronics evidence: Electronic evidence is now vital when dealing with cybercrime investigation by the courts and other legal authorities. Using such evidence pose several challenges but also creates new methods for combatting cybercrime. For cases that have only electronic pieces of evidence, the ability to effectively detect and prosecute a criminal may depend on the right collection and assessment of electronic evidence. While the conventional documents are presented by submitting the original evidence in court, digital evidence in some cases requires well-defined processes that do not allow conversion into other forms, for example by giving a printing out of the evidence and other documents. Legislation are required for handling the admissibility of evidence in the fight against cybercrime.

International cooperation: Majority of the cybercrime offences have a global dimension due to its transnational nature and the globalisation of services. These gave rise to the three treaties being signed that aid the cooperation of member nations in fast-tracking fighting global cybercrime. They are the extradition treaty, mutual legal assistance and the informal agency-to-agency communication.

 Discussion

How could virtual currency be vulnerable to crime?

4.0 Self-Assessment Exercise(s)

1. Using Nigeria Communication Commission (NCC) as an example of a regulator in fighting cybercrime, explain "facilitation of law enforcement".

   Answer:
   The Nigeria government can authorise NCC as a regulator to areas such as anti-spam when it comes to using internet services from their local internet providers, content regulation for all broadcasting houses and internet providers and, enforcing co-regulatory measures.

2. What is the relevance of crime prevention when punishments already exist for offenders?

   Answer:
   Crime prevention is identified as a critical element in an effective and effifcient fight against cybercrime. This is because fewer resources will be needed for the preventive measure as compared to correcting it.

Group Mini Project (5 person's maximum)
Analyse and discuss national cyber law enforcement efforts to date in Nigeria.
Guide: Ten (10) pages minimum with references using 12 point Times New Roman with a line spacing of 1.5.

5.0 Conclusion

When drafting cybercrime legislation, there is the need to first look at what has worked in other climes and to see whether it can be applied to once country of interest. There might be the need for amendments, updates or changes when adopting existing cybercrime law because of regional differences. Government agencies need to collaborate in drafting and implementing those laws and also to make sure that all stakeholders are

considered when doing this. All key areas must be looked at while setting the benchmarks for those laws.

6.0 Summary

The unit has discussed the trends in cybercrimes legislation. You have seen that regulators are involved in the fight against cybercrime. The cybercrime policy is comparable to a strategy that defines the various tools used to address the issue. Developing a policy enables the country to explain government response to cybercrime problems comprehensively.

7.0 References/Further Reading

Willems, E. (2019). *Cyberdanger: Understanding and Guarding Against Cybercrime.* Springer. Retrieved from https://www.springer.com/gp/book/9783030045302

World Bank; United Nations. (2017). *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies (English).* Washington, D.C.: World Bank Group. Retrieved from http://documents.worldbank.org/curated/en/355401535144740611/Combatting-Cybercrime-Tools-and-Capacity-Building-for-Emerging-Economies